Michigan Telecommunications and Technology Law Review

Volume 10 | Issue 2

2004

From the Cluetrain to the Panopticon: ISP Activity Characterization and Control of Internet Communications

Eric Evans
University of Michigan Law School

NOTE

FROM THE CLUETRAIN TO THE PANOPTICON: ISP ACTIVITY CHARACTERIZATION AND CONTROL OF INTERNET COMMUNICATIONS

*Eric Evans**

Cite as: Eric Evans, *From the Cluetrain to the Panopticon: ISP Activity Characterization and Control of Internet Communications*, 10 MICH. TELECOMM. TECH. L. REV. 445 (2004), *available at* http://www.mttlr.org/volten/Evans.pdf

* J.D., University of Michigan Law School, 2004; A.M. in Regional Studies-Middle East, Harvard University, 1997; A.B. in Near Eastern Civilizations, Harvard University, 1993. The author would like to thank Professor Molly Van Houweling for her invaluable guidance and support during the research and writing of this Note.

INTRODUCTION

> 6. The Internet is enabling conversations among human beings that were simply not possible in the era of mass media.
>
> 7. Hyperlinks subvert hierarchy.
>
> 8. In both *inter*networked markets and among *intra*networked employees, people are speaking to each other in a powerful new way.
>
> 9. These networked conversations are enabling powerful new forms of social organization and knowledge exchange to emerge.
>
> *The Cluetrain Manifesto*[1]

> [T]he more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose X of the establishment have been attained. Ideal perfection, if that were the object, would require that each person should actually be in that predicament, during every instant of time. This being impossible, the next thing to be wished for is, that, at every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he should *conceive* himself to be so.
>
> Jeremy Bentham, *The Panopticon Writings*[2]

One important aspect of Internet communications' value to society is the zone of social and technical freedom that the Internet creates.[3] These arguments assume that end users[4] can treat the Internet as a cloud net-

---

1. CHRIS LOCKE, DOC SEARLS, & DAVID WEINBERGER, THE CLUETRAIN MANIFESTO, *at* http://www.cluetrain.com/#manifesto (April, 1999). The Cluetrain Manifesto consists of 95 "theses" which purport to describe and define the dynamics of a markets characterized by non-hierarchical information flow.

2. JEREMY BENTHAM, THE PANOPTICON WRITINGS 29–95 (Miran Bozovic ed., Verso 1995) (1787).

3. *See supra* note 1. Legal scholarship arguing for the transformational potential of Internet communications includes LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books 1999) and Yochai Benkler, *Overcoming Agoraphobia: Building the Commons of the Digitally Networked Environment*, 11 HARV. J.L. & TECH. 287 (1998). Alternative theories that purport to explain the Internet's transformational potential are legion; they lie, however, beyond the scope of this Note.

4. For purposes of this Note, the author will use the term "end user" to refer to a natural person who makes use of Internet communications facilities to communicate with another natural person or automated instrumentality. This use of end user corresponds closely to the term "user" or "user of the system or network" that appears in 17 U.S.C. § 512(b)–(d) (2002), though section 512's definition does not exclude automated instrumentalities.

work whose topology is so complex that the routes that information takes are unimportant or at least unprofitable to worry about.[5] They also assume that communications over the Internet are unknowable in technical terms and legally shielded from routine monitoring. If these assumptions are true, end users—citizens if one conceives of them as political subjects, consumers in an economic sense—have the ability to create social and technological communities that ignore physical and network topology and to share information according to their desires. This increase in the availability of information tends in the aggregate to increase the efficiency of markets.

Direct control over communications over the Internet rests with the Internet service providers (ISPs)[6] who own the individual networks that, in the aggregate, comprise the Internet. The effectiveness of this confederation of networks rests on ISPs' decisions to adopt a particular suite of standard networking protocols—Internet Protocol (IP)[7] and Transport Control Protocol (TCP) are its highest-profile members—that allow end users to be indifferent to the configuration of the networks between their computers. IP, in particular, operates on the assumption that any computer that receives a communication will forward that message to the next computer on the route to its ultimate destination.[8] So far, participants in large IP networks have generally transmitted other participants' messages without further examination of their source or content, exactly

5. For an early and authoritative description of this characteristic of the Internet, see A. MARINE, J. REYNOLDS, AND G. MALKIN, RFC 1594, ANSWERS TO COMMONLY ASKED "NEW INTERNET USER" QUESTIONS (1994), *available at* http://www.ietf.org/rfc/rfc1594.txt?number=1594 (characterizing Internet as "a collection of thousands of networks linked by a common set of technical protocols which make it possible for users of any one of the networks to communicate with or use the services located on any of the other networks. These protocols are referred to as TCP/IP or the TCP/IP protocol suite.").

6. For purposes of this Note, the author will use the term "ISP" to refer to entities that meet 17 U.S.C. § 512(k)(1)(A)'s definition of service provider: "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." The author will refer to entities that meet 17 U.S.C. § 512(k)(1)(B)'s more generous definition—"provider of online services or network access, or the operator of facilities therefor"—as "service providers." As 17 U.S.C. § 512(k)(1)(B) provides, all ISPs are therefore also service providers. The exposure of section 512(k)(1)(B) service providers to liability for their users' copyright infringement lies beyond the scope of this Note.

7. This Note will use the acronym "IP" to refer to Internet Protocol as opposed to intellectual property.

8. *See, e.g.*, DEFENSE ADVANCED RESEARCH PROJECT AGENCY (DARPA), RFC 791, INTERNET PROTOCOL 2 (J. Postel, ed., 1981) *available at* http://www.ietf.org/rfc/rfc0791.txt?number=0791 (describing the operation of IP networks connected by gateways or routers that forward information from local network to local network).

as if they were common carriers.[9] This rule of universal mutual message forwarding is essential to Internet end users' ability to create and use sophisticated communications applications without concerning themselves with the details of the network routes that connect their computers.[10] Universal mutual message forwarding requires ISPs to act more or less as common carriers; they forward messages without regard for their origin, destination, or content.[11]

Despite the fact that they generally behave as common carriers, ISPs are not generally entitled to the blanket protection from liability for forwarding others' messages granted to common carriers such as telecommunications providers.[12] Instead, in the vital area of protection from liability for users' copyright infringement, ISPs are subject to a complex set of rules enumerated in 17 U.S.C. § 512.[13] These rules require courts to characterize the ISP's activities as (a) transmission or routing, (b) system caching, (c) storage of material at a user's direction, or (d) providing an information location tool in order to determine which set of liability protections apply.[14] The court's characterization of the ISP's activity will also determine whether a copyright holder may serve subpoenas under section 512(h) requiring the ISP to identify the user who originated the allegedly infringing message as well as the extent of injunctive relief available under section 512(j).[15] A court's characteriza-

---

9. For an extensive discussion of the importance of the default rule that operators of large IP networks will automatically forward messages passed to them by other operators of large IP networks, see Jonathan Zittrain, *Internet Points of Control*, 44 B.C.L. REV. 653, 655–58 (providing general description of IP routing among operators of large IP networks).

10. There are, of course, exceptions to the rule of universal forwarding, but it is the basic characteristic that defines the Internet. ISPs refer to refusal to forward communications for a particular source as the "Internet death penalty" and reserve it for other ISPs who transmit large amounts of unsolicited commercial email or other undesirable communications. *See* THE JARGON LEXICON 4.3.3: INTERNET DEATH PENALTY, *at* http://jargon.watson-net.com/jargon.asp?w=Internet+Death+Penalty (last visited September 20, 2002).

11. For further discussion of the common carrier doctrine, see discussion *infra* Part I.B.ii.

12. *See, e.g.*, 47 U.S.C. § 153(10) (2002) (definition of common carrier in context of telecommunications regulation); *see also* discussion *infra* Part I.B.ii. Note that because many ISPs—BellSouth, MCI, SBC, AT & T, and Verizon, for example—are also full-blown common carriers with respect to their telecommunications activities, they will be subject to different rules of liability depending on the nature of the traffic that flows over their lines. The difficulties of reconciling the common carrier and ISP elements of these entities, especially with the emergence of voice-over-IP technology, lie beyond the scope of this Note.

13. 17 U.S.C. § 512 (2002).

14. *See id.* § 512(a)–(d) (enumerating safe harbors from liability); *see also* discussion *infra* Part II.A.

15. *See id.* § 512(h), (j) (enumerating requirements for subpoena requiring ISP to identify user who originated allegedly infringing material and limiting injunctive relief available where ISP engaged in routing and transmission); *see also* Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1236 (D.C. Cir. 2003) (holding that section

tion of an ISP's activity therefore determines whether the activity exposes the ISP to liability and whether the identity of the other party is easily discovered.[16]

If a court characterizes the ISP's activity as transmission or routing, the ISP is effectively shielded from direct and contributory liability for its users' copyright infringement[17] and the copyright holder is not entitled to a section 512(h) subpoena requiring the ISP to identify the alleged offender.[18] If the court characterizes the ISP's activity in any other way, the ISP is exposed to contributory liability for its users' activities[19] and the copyright holder may serve a section 512(h) subpoena.[20] Courts have not reached a consensus on how to characterize particular activities, and the statute and its legislative history provide only limited guidance.[21] In a particularly important example of the difficulties that section 512's characterization scheme raises, different courts have characterized ISP participation in Usenet—a mutual message forwarding network detailed *infra* in Part I.B.iii—as transmission and forwarding and as storage of material at a user's direction.[22] The courts' characterization of ISP participation in Usenet decisively shaped the parties' options in later litigation.[23] Courts' inconsistency in characterizing Usenet for section 512 purposes raises the possibility that courts may characterize other mutual message-forwarding systems inconsistently, leaving ISPs uncertain of their exposure to liability if they participate or allow their users to participate in these systems.

If ISPs are exposed to liability for forwarding others' messages—messages originating with other ISPs or with the ISP's own users—the norm of universal mutual message forwarding that underlies the present operation of the Internet will be threatened.[24] This Note will argue that

---

512(h) subpoena unavailable where ISP acts as a mere conduit for transmission or routing but available in other cases).

16. *See* discussion *infra* Parts II.A.vi, II.B.

17. Assuming that the ISP has met the threshold requirements for safe harbor contained in 17 U.S.C. § 512(i). For further development of this point, see discussion *infra* Part II.B.

18. *See* discussion *infra* Part II.A.vi.

19. *See* discussion *infra* Part II.A.vi.

20. *See* discussion *infra* Part II.A.vi.

21. *See* discussion *infra* Parts II.B, III.A.

22. *Compare* Ellison v. Robertson, 189 F. Supp. 2d 1051 (C.D. Cal. 2002), *appeal docketed*, No. 02-55797 (9th Cir. argued Mar. 6, 2003), *with* ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001). *See also* discussion *infra* Parts III.A.

23. *See* discussion *infra* Part III.A.

24. The norm of universal mutual message forwarding that characterizes the Internet is already under threat from a number of technical and political developments, including the extensive use of Network Address Translation (NAT) to conserve IP addresses, security filtering, and non-US government regulation barring the use of particular applications, such as Voice Over IP (VoIP or Internet telephony). *See, e.g.*, David L. Margulius, *Trouble on the Net*,

society presently confronts a choice between a common carrier Internet characterized by universal mutual message forwarding and a monitored and controlled Internet. Part I will describe the underlying rules that govern ISPs' liability for their users' actions. Part II will argue that the present statutory regime governing ISPs' liability for users' copyright infringement includes elements that provide ISPs with substantial protection for mutual message forwarding and that this regime relies on courts to characterize ISPs' activities to determine which liability standard applies. Part III will argue that courts have characterized one particular networking activity—participating in the Usenet message-forwarding system—inconsistently and that ISPs have not been able to predict the degree to which forwarding Usenet messages exposes them to liability. Part IV will argue that characterizing ISPs' activities so that ISPs are exposed to secondary liability, obliged to comply with section 512(h) subpoenas, and denied section 512(j)(2)'s limits on injunctive relief will undercut the norm of universal mutual message forwarding that allows Internet communication and urge courts to characterize ISP activity as transmission or routing protected by the section 512(a) safe harbor to avoid these negative effects.[25]

I. THE DMCA COMPROMISE

The present regime governing ISPs' liability for copyright infringement on the part of their end users is defined in Title II of the Digital Millennium Copyright Act (DMCA) of 1998, codified in 17 U.S.C. § 512.[26] These provisions exist in the context of two important legal regimes: the legal regime governing copyright infringement and the legal regime governing electronic communications. Analyzing 17 U.S.C. § 512 independently of this broader context risks creating inconsistencies between the regimes governing particular genera of electronic communications. Part I.A will quickly summarize copyright infringe-

---

INFOWORLD, Nov. 24, 2003, at 40, 42–43. These technological and policy issues lie outside the scope of this Note.

25. This Note will focus on the issues of direct and contributory liability for copyright infringement and copyright holders' authority to issue section 512(h) subpoenas only; the issue of vicarious liability, while extremely important to defining ISPs' comprehensive liability exposure, will arise only in passing.

26. Digital Millenium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998). For a recent discussion of the liability regime created in the DMCA, see Raphael Guiterrez, *Save The Slip For The Service Providers: Courts Should Not Give Short Shrift To The Safe Harbors Of The Digital Millennium Copyright Act*, 36 U.S.F.L. REV. 907 (2002); for a less serious, but more insightful, analysis, see also David Nimmer, *Back from the Future: A Proleptic Review of the Digital Millennium Copyright Act*, 16 BERKELEY TECH L.J. 855 (2001).

ment doctrine. Part I.B will describe the legal regimes governing copyright infringement, electronic communications privacy and communications service provider liability in general. Part I.B will also argue that these overall norms shaped Congress's decision to provide ISPs with robust protection from liability for forwarding others' messages in section 512(a).

A. *Copyright Infringement and Liability*

Under normal circumstances, anyone who violates an exclusive right of a copyright holder is liable for copyright infringement.[27] The exclusive rights of copyright holders include the right to reproduce a copyrighted work, the right to distribute the work, the right to display the work publicly, and the right to perform the work publicly.[28] Any electronic communication that includes unlicensed copyrighted works will violate these exclusive rights. Routers and cache servers, for example, produce reproductions of every packet they receive. Computer monitors must display or perform a work for a user to view it.[29]

In addition, parties who materially contribute to infringement by another with actual or constructive knowledge of that infringement will be liable for contributory infringement.[30] The consensus opinion of courts is that ISPs who engage in passive, automatic copying of copyrighted works incident to forwarding others' messages are not liable for direct infringement.[31] In the absence of statutory protection, however, ISPs may be liable for contributory infringement where they have actual or constructive knowledge of the infringement, since their passive, automatic copying qualifies as material contribution to infringement.[32] Courts will

---

27. *See* 17 U.S.C. § 501 (2002).

28. *See* 17 U.S.C. § 106 (1), (3)–(5) (2002).

29. *See, e.g.,* Kelly v. Arriba Soft Corp., 336 F.3d 811, 817 (9th Cir. 2003) (holding that creation of thumbnail images violates owner's reproduction right); Religious Tech. Ctr. v. Netcom, Inc., 907 F. Supp. 1361, 1367 (N.D. Cal. 1995) (describing reproduction of copies of copyrighted works necessary to operation of Internet).

30. *See* Gershwin Pub. Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019 (9th Cir. 2001).

31. *See Netcom*, 907 F. Supp. at 1372–73 (holding ISP not directly liable for passive, automatic copying incident to forwarding others' messages); *see also* ALS Scan v. RemarQ Communities, Inc., 239 F.3d 619, 622 (4th Cir. 2001) (following *Netcom* on issue of direct infringement by ISP); Ellison v. Robertson, 189 F. Supp. 2d 1051, 1057 (C.D. Cal. 2002) (following *Netcom* on issue of direct infringement by ISP); *but see* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993) (holding BBS provider liable for passive, automatic copying incident to forwarding users' messages).

32. *See Netcom*, 907 F. Supp. at 1375 (holding that "[p]roviding a service that allows for the automatic distribution of all Usenet postings, infringing and noninfringing" satisfies material contribution element of contributory infringement); *Ellison*, 189 F. Supp. 2d at 1058 (adopting *Netcom* conclusion that "[p]roviding a service that allows for the automatic

not, however, impute constructive knowledge of infringement to the manufacturer of a technology with substantial non-infringing uses based on the capability of the technology to allow infringement.[33]

B. *Privacy and Service Provider Liability in General*

In general, electronic communications are accorded a high level of protection from monitoring by the state or other interested private parties.[34] Also, telecommunications services are generally shielded from liability for the communications that travel over their networks based on their status as "common carriers."[35] A common carrier is a service provider, such as a railroad, electric utility, or telecommunications provider, which makes its facilities available to all comers and exercises limited control over the use of its services.[36] Common carriers are not liable for the actions other parties take using their services.[37]

1. The Electronic Communications Privacy Act (ECPA) (18 USC §§ 2510 et seq.)

The Electronic Communications Privacy Act (ECPA),[38] initially passed in 1968[39] and extensively revised in 1986, extends statutory pro-

---

distribution of all Usenet postings, infringing and noninfringing" when ISP has knowledge of infringement constitutes contributory infringement).

33. *See Napster*, 239 F.3d at 1022.

34. *See* discussion *infra* Part I.B.i.

35. *See generally* Anderson v. New York Tel. Co., 320 N.E.2d 647, (N.Y. 1974) (applying common carrier liability protection to telephone service provider); People v. Lauria, 251 Cal. App. 2d 471 (1967) (applying common carrier liability limitation to telephone answering service).

36. *See* Nat'l Ass'n of Regulatory Util. Comm'rs v. F. C. C., 533 F.2d 601, 608–09 (D.C. Cir. 1976), which states:

> [T]he primary *sine qua non* of common carrier status is a quasi-public character, which arises out of the undertaking 'to carry for all people indifferently.' This does not mean that the particular services offered must practically be available to the entire public; a specialized carrier whose service is of possible use to only a fraction of the population may nonetheless be a common carrier if he holds himself out to serve indifferently all potential users. Nor is it essential that there be a statutory or other legal commandment to serve indiscriminately; it is the practice of such indifferent service that confers common carrier status. That is to say, a carrier will not be a common carrier where its practice is to make individualized decisions in particular cases whether and on what terms to serve.

37. *See* discussion *infra* Part II.B.ii

38. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C., including 2510–21, 2701–10, 3121–26).

39. *See* Electronic Communications Privacy Act of 1968, Pub. L. No. 90-351 § 802, 82 Stat. 212 (1968).

tection to the content of electronic communications.[40] ECPA protects all "wire, oral, or electronic communication," including Internet communication over an ISP's cable and routers.[41] ECPA places strict limits on ISPs' ability to monitor and control their networks in order to preserve the privacy of communications over those networks.[42] ISPs—and all other persons—are prohibited from interception and random monitoring of the content of telephone and other electronic communications.[43] Providers and their employees are subject to criminal liability if they intercept, disclose, or use the content of any such communication except in the course of providing service.[44] Telecommunications providers, including ISPs, may not engage in random monitoring except for quality control purposes.[45]

Similar, though less stringent, provisions cover disclosure of the content of stored electronic communications, such as email messages stored on an ISP's mail server. 18 U.S.C. § 2703(a) requires a warrant issued by a magistrate before an ISP may disclose the contents of a subscriber's stored communications to the government.[46] ISPs need not

---

40. A full treatment of the intricacies of ECPA lies beyond the scope of this Note. The limited treatment here does not fully address the "fog of inclusions and exclusions" created by ECPA. Briggs v. Am. Air Filter, 630 F.2d 414, 415 (5th Cir. 1980).

41. 18 U.S.C. § 2511(1) (2002). ECPA uses "wire communication" to refer to conventional telephone communication: "any aural transfer made in whole or in part through the use of facilities for the transmission of communication by the aid of wire, cable, or other like connection. . . ." *Id.* § 2510(1).

42. *See id.* § 2511(1) ("(1) Except as otherwise specifically provided in this chapter any person who— (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication. . . .")

43. *Id.*

44. *See id.* § 2511(1)(a)–(c) (prohibiting interception, use, and disclosure).

45. Providers may disclose any information intercepted during routine monitoring. *See id.* § 2511(2)(a)(i).

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, *except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.*

Id. (emphasis added). ISPs clearly fall within 18 U.S.C. § 2510(15)'s definition of a provider of electronic communication service: a provider of "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15).

46. *See id.* § 2703(a) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant. . . .").

disclose "record[s] or other information pertaining to a subscriber" beyond the subscriber's name, address, and payment arrangements without a search warrant.[47] ISPs may—but need not—disclose information about subscribers, but not the content of their electronic communications, to non-governmental entities.[48] These provisions preserve the confidentiality of electronic communications and reflect a strong societal interest in protecting the privacy of electronic communications, though they serve primarily to protect electronic communications against interception in transit.

2. The Common Carrier Doctrine as Applied to Telecommunications Providers and ISPs

These restrictions on telecommunications providers' freedom to monitor communications reduce their ability to prevent infringing uses of their networks. The limited control that conventional telecommunications providers may exercise over their subscribers has led Congress to provide them with statutory protection from liability for copyright infringement in cases where they have no control over the information transmitted over their networks and do no more than provide transmission facilities.[49] This statutory protection is closely analogous with the liability protection courts have offered to other sorts of common carriers under the common carrier doctrine.[50]

The common carrier doctrine is available to ISPs as well as to conventional telecommunications service providers. Congress and the courts have applied the common carrier doctrine to ISPs in cases involving defamation. In *Cubby v. Compuserve*,[51] a court refused to

---

47. *See id.*

48. *See id.* § 2702(c)(5).

49. *See* 17 U.S.C. § 111(a)(3) (2002).

> (a) The secondary transmission of a performance or display of a work embodied in a primary transmission is not an infringement of copyright if . . .
>
> (3) the secondary transmission is made by any carrier who has no direct or indirect control over the content or selection of the primary transmission or over the particular recipients of the secondary transmission, and whose activities with respect to the secondary transmission consist solely of providing wires, cables, or other communications channels for the use of others: Provided, That the provisions of this clause extend only to the activities of said carrier with respect to secondary transmissions and do not exempt from liability the activities of others with respect to their own primary or secondary transmissions . . . .

Id.

50. *Compare id. with* Nat'l Ass'n of Regulatory Util. Comm'rs v. F. C. C., 533 F.2d 601, 608–09 (D.C. Cir. 1976). *See also supra* note 36 and accompanying text.

51. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

impose liability on an ISP for statements a user had distributed in one of its chat rooms.[52] The court applied the common carrier doctrine in order to prevent potential liability for defamation from imposing "an undue burden on the free flow of information."[53] Congress endorsed the court's decision in the Communications Decency Act (CDA),[54] which extends statutory protection from liability for defamation where another party originates the allegedly defamatory speech.[55] In doing so, it explicitly found that the diversity of political discourse on the Internet and the unique opportunities for cultural development that it provided were closely related to limited state and federal regulation of the medium.[56] Courts have consistently applied the common carrier doctrine in post-CDA defamation cases.[57] In *Zeran v. America Online*, for example, the Fourth Circuit explicitly mentioned Congress's findings in the CDA in refusing to impose liability on an ISP for allegedly defamatory material posted by a subscriber.[58] The court noted that "[t]he imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech."[59] Later courts have adopted the same rule,

52. *See id.* at 140. ("A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information.").

53. *Id.*

54. Communications Decency Act of 1996 (DCA), Pub. L. No. 104-104, 110 Stat. 56 (1996).

55. *See* 47 U.S.C. § 230 (2002) ("No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider.").

56. *See id.* § 230(a), (b) (finding, *inter alia*, that "[t]he Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity," that "[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation," and declaring the policy of the United States to be "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation").

57. *See, e.g.*, Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) ("Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering 'a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.' "); Blumenthal v. Drudge, 992 F. Supp. 44, 49–50 (D.D.C. 1998) (applying 47 U.S.C. § 230 to shield service provider from liability for allegedly defamatory gossip column); Noah v. AOL Time Warner, Inc., 261 F. Supp. 2d 532, 537–38 (E.D. Va. 2003).

58. *Zeran*, 129 F.3d at 330.

59. *Id.*

shielding ISPs and other "provider[s] . . . of . . . interactive computer service[s]" from liability for defamatory material posted by subscribers.[60]

3. Pre-DMCA ISP Liability for Copyright Infringement

While courts were relatively uniform in their treatment of ISP liability for defamation by users, no such uniformity emerged with respect to ISP liability for users' copyright infringement. Before the passage of the DMCA in 1998 created a statutory scheme governing service providers' liability for users' copyright infringement, courts were divided in their approaches.

One approach, typified by *Playboy Enterprises, Inc. v. Frena*,[61] found ISPs directly liable for users' copyright infringement.[62] In *Frena*, a local BBS provider allowed paid subscribers to store graphics files on the BBS' computer.[63] Other paid subscribers of the BBS could then transfer copies of these graphics files to their own computers.[64] The opinion includes no information on whether the BBS forwarded communications to other networks.[65] A subscriber of the BBS stored graphics files that infringed plaintiff's copyrights on the BBS; other subscribers then downloaded the files.[66] The BBS played no role in selecting the files stored on its equipment and took affirmative steps to disable access to the files after receiving notice of the infringement, including policing users' activities to prevent future infringement.[67] During this course of events, the BBS' equipment generated copies of the infringing material incidental to its automated response to requests for the files initiated by subscribers.[68] Playboy brought suit against the BBS provider for copyright infringement, among other claims.[69]

The *Frena* court reasoned that generation of copies—at one's own initiative or at the request of another party—sufficed to establish direct copyright infringement; the BBS owner's intent to infringe and ability to prevent infringement were irrelevant.[70] The *Frena* court did not address

---

60. *Blumenthal*, 992 F. Supp. at 52–53 (explicitly adopting *Zeran* court's analysis of section 230); *see also Noah*, 261 F. Supp. 2d at 537–38 (explicitly adopting *Zeran* court's analysis of section 230).

61. Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).

62. *Id.* at 1556.

63. *Id.* at 1554.

64. *Id.*

65. *See id.*

66. *Id.*

67. *Id.*

68. *Id.* at 1556.

69. *Id.* at 1554.

70. *See id.* at 1559 ("It does not matter that Defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not an element of infringement, and thus even

the possibility that the BBS might qualify as a common carrier. As a small, subscription-only service that did not forward messages for other network providers, its claim to such status would have been weak at best.

The *Frena* approach became unworkable as the volume of messages and later commerce that flowed over computer networks increased. A legal regime in which every intermediate party involved in the automatic forwarding of an infringing message was directly liable for copyright infringement would impose crushing liability exposure on every major ISP. For this reason, courts soon rejected the *Frena* approach for an approach that shielded ISPs from most liability. This approach, exemplified by *Religious Technology Center v. Netcom, Inc.*,[71] refused to find ISPs *directly* liable for users' copyright infringement where the actual copying resulted from the automatic functioning of the ISP's equipment, but left open the possibility that the ISP might be contributorily liable if it "knew of any infringement . . . before it was too late to do anything about it."[72] In *Netcom*, Netcom, an ISP, provided Internet access to a bulletin board system (BBS) operated by another party; this BBS provided its end users with access to a Usenet server.[73] The services Netcom provided to the BBS included access to Netcom's Usenet server, which automatically forwarded messages to other Usenet servers according to rules Netcom defines.[74]

Usenet is an automated system for distributing messages across the Internet and, in some cases, other networks.[75] These messages are organized according to several criteria:

> Usenet . . . consists of a set of "newsgroups" with names that are classified hierarchically by subject. "Articles" or "messages" are "posted" to these newsgroups by people on computers with the appropriate software—these articles are then broadcast to other interconnected computer systems via a wide variety of networks.[76]

---

an innocent infringer is liable for infringement. . . ."). Since the plaintiff had established direct copyright infringement, the court did not address contributory liability.

71. Religious Tech. Ctr. v. Netcom, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

72. *Netcom*, 907 F. Supp. at 1372 (refusing to impose direct liability on ISP for automatic copying and transmission of plaintiff's copyrighted work at direction of user); *id.* at 1374.

73. *Id.* at 1366.

74. *Id.* at 1367.

75. For a general discussion of Usenet, see WIKIPEDIA, THE FREE ENCYCLOPEDIA, *at* http://en2.wikipedia.org/wiki/Usenet (last updated Dec 3, 2003); for a slightly outdated but still valuable discussion of Usenet and Usenet culture, see Mark Moraes, *What is Usenet?*, *at* http://www.faqs.org/faqs/usenet/what-is/part1/ (last updated Jan 16, 1998).

76. *Netcom*, 907 F. Supp. at 1367.

Usenet, with its decentralized administrative structure, worldwide end user community, and strong cultural traditions of anarchic independence includes newsgroups ranging from the harmless oddity of alt.swedish.chef.bork.bork.bork to the serial-killer-fan discussion of alt.fan.karla-homolka to channels for distribution of obscene and illegal images like the cryptically-named alt.binaries.adolescents.off-topic.[77]

Usenet servers forward messages to each other according to rules established on every server; some servers refuse messages from particular newsgroups, by particular authors, in particular hierarchies, or based on other criteria.[78] Each server has a set of rules defined by its owner and accepts and forwards messages based on those rules. The process is automated in that humans set the rules for forwarding and accepting messages; the application of the rules is left to the automated instrumentality of the server.

Servers retain only a single copy of each message and distribute it to end users on demand. This method of distributing messages reduces the amount of network capacity that Usenet servers and end users consume in distributing messages throughout the network of Usenet servers.

Usenet servers retain end users' messages for a period of time determined by the local system administrator. Because of the high volume of traffic on Usenet, most system administrators limit retention of messages to two weeks or less. Newsgroups that generate a high volume of data—especially those in which binary files such as compiled computer programs or graphics files—will often have shorter retention periods. Some Usenet servers will have longer retention periods, ranging up to the indefinite retention period of Usenet archives such as Google Groups.[79]

Many ISPs maintain Usenet servers for their subscribers. Some Usenet servers have particularly permissive rules; these servers will often charge a separate fee for access. End users gain access to Usenet by connecting to a server using a client program. Such client programs are called "newsreaders." End users generally do not participate in Usenet by hosting a server themselves.

---

77. Usenet's decentralized structure makes it effectively impossible to create a definitive list of existing groups. For a sample list of the 10,635 groups in the alt hierarchy carried by UUNet, a major ISP, as of Feb. 23, 2000, see http://www.itc.virginia.edu/~rlb0p/uunet.alt.txt.

78. For a full discussion of the categories of information that may be used to differentiate among Usenet messages, see Memorandum from M. Horton & R. Adams, RFC 1036—Standard for Interchange of USENET Messages, at http://www.ietf.org/rfc/rfc1036.txt (last visited April 15, 2004).

79. Google Groups' Usenet archive is available at http://groups.google.com.

In *Netcom*, an end user of the BBS infringed the Religious Technology Center's (RTC's) copyrights by calling into the BBS and posting a message containing copyrighted texts including secrets of the Church of Scientology to its Usenet server.[80] The BBS' Usenet server then automatically forwarded the message to Netcom's Usenet server.[81] Netcom's Usenet server, in turn, automatically forwarded the message to other Usenet servers before deleting it.[82] The infringing end user had no contractual relationship with Netcom.[83]

RTC informed both the BBS and Netcom of the end user's infringing activity but neither party took action to stop him; Netcom claimed that it lacked sufficiently fine-grained control over its network to stop a single end user's messages.[84] RTC then filed a complaint claiming that Netcom was liable for the end user's copyright infringement on both direct and contributory theories.[85]

The *Netcom* court found that Netcom was not directly liable for copyright infringement on the part of the end user because it had not initiated the copying: "the mere fact that Netcom's system incidentally makes temporary copies of plaintiffs' works does not mean Netcom has caused the copying."[86] Under these circumstances, the court found that Netcom had acted "like a conduit" in that it forwarded messages at the direction of another.[87] The court, however, explicitly declined to extend the common carrier doctrine to ISPs[88] and therefore left them open to contributory liability.[89]

The court's contributory liability analysis focuses almost entirely on the knowledge element because the automated copying of the infringing material, while not sufficient to establish direct liability, was sufficient to satisfy the material contribution element of contributory liability.[90] The

80. *Netcom*, 907 F. Supp. at 1367.

81. *Id.* at 1367 (outlining chain of transmission of end user's messages).

82. *Id.* (noting that Netcom retained the message for eleven days).

83. *Id.* at 1367–68.

84. *Id.* at 1366.

85. *Id.* (Plaintiff's claim included the end user and BBS as defendants in addition to Netcom.)

86. *Id.* at 1369.

87. *Id.* at 1372.

88. *See id.* at 1369 n.12 (extensively discussing common carrier doctrine and concluding that ISPs are not common carriers because they provide more than "the wire and conduits" for the infringing activity and 17 U.S.C. § 111(a)(3) explicitly limits common carrier protection to entities that satisfy both that condition and also exercise no control over the content of the communications over their networks).

89. *See id.* at 1373 (holding that Netcom may be liable for contributory infringement).

90. *See id.* at 1375 (holding that forwarding potentially-infringing messages "goes well beyond" satisfying material contribution element of contributory liability).

court treats knowledge of infringement and the ability to prevent the infringement as if they are identical—an assumption that may not have been justified given the prevailing standard of technology at the time but may be more justified now.[91] The court concluded that an ISP will be contributorily liable for copyright infringement initiated by a user when it "[knows] of any infringement . . . before it was too late to do anything about it."[92] The court appears to have assumed the ISPs would not, in fact, be subject to contributory liability, since the prevailing technology did not allow fine-grained knowledge of traffic patterns:

> Billions and billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from noninfringing bits. Because the court cannot see any meaningful distinction (without regard to knowledge) between what Netcom did and what every other Usenet server does, the court finds that Netcom cannot be held liable for direct infringement.[93]

While the court is addressing the issue of direct infringement, its assumption that ISPs will not be able to identify and stop infringing activity makes it extremely unlikely that any ISP operating under the then-prevailing technological standard would ever know of infringement "before it was too late to do anything about it." If an ISP can never "do anything about it," knowledge of infringement will always arrive too late. Despite its refusal to adopt the common carrier doctrine directly, the *Netcom* standard, with its combination of a "conduit" protection from direct liability and limited knowledge and control as a shield against contributory liability, provided ISPs with protection from direct and contributory liability for users' copyright infringement. Courts tended to follow *Netcom* and refuse to impose direct or contributory liability without some level of knowledge of infringement or intent to infringe on the part of the ISP.[94]

---

91. *See, e.g., id.* at 1372 (noting that "no purpose would be served by holding liable those who have no ability to control the information to which their subscribers have access"); *id.* at 1374 (noting in discussion of knowledge element that Netcom "retains some control over the use of [its] system").

92. *Id.*

93. *Id.* at 1372–73.

94. *See, e.g.*, Playboy Enters., Inc. v. Russ Hardenburgh, 982 F. Supp. 503, 512–14 (N.D. Ohio 1997) (citing *Netcom* approvingly, but finding defendant liable because he became 'active participant' in infringement by inducing subscribers to upload copyrighted works onto its system and exercising editorial control over content); Marobie-FL, Inc. v. NAFED and Northwest Nexus, Inc., 983 F. Supp. 1167, 1178 (N.D. Ill. 1997) (citing *Netcom* approvingly, and finding web hosting service that stored infringing material not liable because it "only

II. TITLE II OF THE DMCA: STATUTORY SAFE HARBOR FOR ISPS

Faced with the conflicting results in *Netcom* and *Frena*, ISPs and representatives of copyright holders pushed for Congressional legislation to define ISPs' liability for infringement on the part of their subscribers. Congress responded to this pressure with Title II of the DMCA. Congress held extensive hearings during drafting of the DMCA and in its final form the legislation enjoyed wide support.[95] Title II of the DMCA, defining the limits of liability protection—the "safe harbors" from liability—for ISPs and other entities that provide services over the Internet, is embodied in 17 U.S.C. § 512.[96] Congress substantially extended the *Netcom* court's rejection of strict liability for direct infringement and refused to hold ISPs liable for copyright infringement incident to their role as conduits for other ISPs' and end users' messages.[97] Part II.A will argue that the text, structure, and legislative history of section 512's limitations of liability for service providers prove that Congress intended to give ISPs a blanket safe harbor from liability for forwarding others' messages. Part II.B will argue that, in their entirety, section 512's provisions extend substantial protection from liability to ISPs whose activities fall into the section 512(a) transmission and routing safe harbor. Part II.C will argue that Congress considered and rejected the option of merely codifying existing case law.

A. *Extending Netcom: Section 512's Safe Harbors*

In Title II of the DMCA, Congress created a series of four safe harbors—particular categories of conduct for which properly-qualified service providers will not be liable for direct, contributory, or vicarious

---

provided the means to copy, distribute or display plaintiff's works, much like the owner of a public copying machine used by a third party to copy protected material").

95. *See* S. REP. NO. 105-190, at 9 (1998) (noting unanimous support for DMCA in Judiciary Committee and broad support from concerned interest groups).

96. For general discussion of section 512's provisions, see Jonathan Band & Matthew Schruers, *Safe Harbors Against The Liability Hurricane: The Communications Decency Act And The Digital Millennium Copyright Act*, 20 CARDOZO ARTS & ENT. L.J. 295 (2002); Jonathan A. Friedman, Esq. & Francis M. Buono, Esq., *Using The Digital Millennium Copyright Act To Limit Potential Copyright Liability Online*, 6 RICH. J.L. & TECH. 18 (2000).

97. *Compare* Religious Tech. Ctr. v. Netcom, Inc., 907 F. Supp. 1361, 1372–73 (N.D. Cal. 1995) (noting that "it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet"), *with* S. REP. NO. 105-190, at 8–9 (1998) (noting the ISPs "must make innumerable electronic copies by simply transmitting information over the Internet"). *See also* 17 U.S.C. § 512(a) (2002).

infringement.[98] Congress intended these safe harbors neither to increase nor to decrease service providers' underlying exposure to liability, but only to shield them from monetary remedies for particular acts on the part of their end users or other service providers.[99] Congress intended to preserve incentives for both service providers and copyright owners to "detect and deal with copyright infringements that take place in the digital networked environment."[100]

To meet these expansive and potentially contradictory goals, Congress created a complex, nested network of safe harbors that shield service providers from liability where the service provider:

1. transmits digital communications across digital networks, (section 512(a))[101] or
2. retains previously-transmitted digital information in temporary storage (section 512(b)),[102] or
3. stores material on its systems or networks at the direction of a user (section 512(c)),[103] or
4. refers or links users to infringing material (section 512(d)).[104]

The safe harbor approach requires courts to characterize a service provider's allegedly infringing activity before it can determine its exposure to liability, the availability of subpoenas to identify an alleged infringer, or the limits imposed on injunctive relief.[105]

i. Threshold Requirements for all Section 512 Safe Harbors

To qualify for safe harbor under any of these provisions, a service provider must "adopt and reasonably implement" a policy that allows it

98. *See* S. REP. NO. 105-190, at 19, 20 (1998) (noting Congressional intent to allow development of service provider liability law, despite creation of categories of subscriber conduct for which service providers are preserved from liability and also noting that safe harbors shield service provider from liability for all monetary relief for direct, contributory, and vicarious infringement). The safe harbor liability protection provisions are extremely complex; the following exposition of its features, while extensive, is necessary to capture the complex interdependencies of its provisions.

99. *See* S. REP. NO. 105-190, at 19, 20 (noting Congressional intent enumeration of safe harbors does not imply expansion or contraction of underlying liability).

100. *Id.* at 20.

101. 17 U.S.C. § 512(a) (2002); S. REP. NO. 105-190, at 41–42.

102. 17 U.S.C. § 512(b); S. REP. NO. 105-190, at 42–43.

103. 17 U.S.C. § 512(c); S. REP. NO. 105-190, at 43–47.

104. 17 U.S.C. § 512(d); S. REP. NO. 105-190, at 47–49.

105. *See* 17 U.S.C. § 512(a)–(d), (h), (j).

to terminate access to its networks and systems for repeat infringers.[106] Each of the safe harbors requires that a service provider meet a number of additional criteria specific to that safe harbor before availing itself of liability protection.

ii. Requirements for Section 512(a) Safe Harbor

The section 512(a) safe harbor applies only to parties that meet section 512(k)(1)(A)'s definition of service provider: "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[107] Section 512(a) shields ISPs that meet section 512(k)(1)(A)'s definition from monetary liability where they use automated means to forward communications originating with other ISPs or dispatched by their own users without altering the content of the communications.[108] The statute expressly rejects the holding in *Frena* and shields ISPs from monetary remedies for making "intermediate and transient [infringing] copies of the information [transmitted] between routers and servers" during its transmission from end user to end user.[109]

The section 512(a) safe harbor closely resembles statutory and common-law liability protection for common carriers in that ISPs may not avail themselves of the section 512(a) safe harbor if they play "an editorial function of determining what material to send, or the specific sources of material to place online . . . rather than 'an automatic technical process' of responding to a command or request, such as one from a user, an Internet location tool, or another network."[110] Congress intended to apply a very broad definition of "editorial function," indicating that service providers who merely selected "the specific sources of material to place online (*e.g.*, a radio station)" would qualify as exercising an editorial function and would therefore not qualify for section 512(a) safe harbor.[111] Section 512(a)'s safe harbor was intended to cover all categories of communications en route from a user to another user; so long as the ISP automatically transmits messages selected and dispatched by

106. *See id.* § 512(i)(1)(A). Section 512(i)(1)(B) imposes the requirement that service providers accommodate and not interfere with standard technical measures to protect copyrighted works. These standard technical measures have not, as yet, materialized.

107. *Id.* § 512(k)(1)(A).

108. *See id.* § 512(a)(1)–(5).

109. S. REP. No. 105-190, at 41 (1998).

110. *Id.* at 42; *see also* 17 U.S.C. § 512(a)(2),(3), (5) (enumerating requirements that service provider seeking section 512(a) safe harbor select neither the recipients of the communication nor the content of the communication).

111. S. REP. No. 105-190, at 42 (discussing 17 U.S.C. § 512(a)(2)).

another person—a user or another network operator—without alteration or selection of the content and does not retain copies of the communication, it will not be liable for monetary damages.[112]

Section 512(a) includes no knowledge element; ISPs that meet the section 512(k)(1)(A) definition and satisfy the requirements of section 512(a)(1)–(5) will qualify for its safe harbor regardless of their state of knowledge regarding the communications.[113] Under section 512(a), so long as an ISP "plays the role of a 'conduit' for the communications of others," it will not be liable for monetary damages for direct, contributory, or vicarious infringement.[114] The section 512(a) safe harbor, therefore, extends ISPs' protection from monetary liability for users' actions beyond the limits of the *Netcom* rule.[115]

iii. Requirements for Section 512(b) Safe Harbor

Section 512(b) shields any organization that meets section 512(k)(1)(B)'s generous definition of "service provider"—"a provider of online services or network access, or the operator of facilities therefor"[116]—from monetary liability for creating intermediate copies of infringing material in a local cache server.[117] So long as the automatic

---

112. *See* discussion *supra*; *see also* 17 U.S.C. § 512(a)(1)–(5).

113. *See* 17 U.S.C. § 512(a)(1)–(5).

114. S. REP. No. 105-190, at 41; *see also id.* at 40 (noting that safe harbors embodied in sections 512(a)–(d) "protect qualifying service providers from liability for all monetary relief for direct, vicarious, and contributory infringement").

115. *Compare id.* at 40 *with* Religious Tech. Ctr. v. Netcom, Inc., 907 F. Supp. 1361, 1373 (N.D. Cal. 1995) (holding that Netcom may be liable for contributory infringement).

116. 17 U.S.C. § 512(k)(1)(B) (2002). Courts have interpreted this definition very broadly; there are, as yet, no decisions which set its limits. eBay, USENET news providers, and AVS providers have all been included within this definition. *See* Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1087 (C.D.Cal. 2001) ("eBay clearly meets the DMCA's broad definition of online 'service provider.'"); *see also* ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 623 (4th Cir. 2001) (holding that USENET news provider meets section 512(k)(1)(B) definition); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1175 (C.D. Cal. 2002) (holding that AVS provider will be treated as section 512(k)(1)(B) service provider for summary judgment purposes).

117. A full discussion of caching is beyond the scope of this Note. Network caching allows a service provider to maximize the efficiency of its low-capacity network link (such as an upstream connection to the Internet) by placing a cache server on the downstream side of the link. When a user of the service provider's network requests a particular item for the first time, the service provider's network will retrieve it for the user over the low-capacity link. The cache server will retain a copy of the item. When another user requests the same item, the service provider's network will deliver the copy stored in cache instead of retrieving the original copy—thus avoiding use of the low-capacity link and reducing the service provider's total cost of maintaining its upstream connectivity. In situations where many users request the same items, caching can substantially reduce service providers' connectivity costs. For additional discussion of network caching, see, for example, White Paper from Cisco Systems, Network

storage and transmission of material on the cache server is initiated by other persons and the service provider neither interferes with copyright management tools nor alters the content of the stored material, the service provider is shielded from monetary liability for infringement.[118]

Section 512(b) includes a very limited knowledge element. In order to qualify for its safe harbor, service providers must remove or disable access to material stored in a network cache if:

1. they receive a formal notice that infringing material is stored on their network cache,[119] and
2. access to the original source of the infringing material has been disabled,[120] and
3. the formal notice includes a statement that access to the original source has been disabled.[121]

Section 512(b) requires no action of service providers unless they receive a notice complying with the requirements above.[122]

iv. Requirements for Section 512(c) Safe Harbor

Congress intended section 512(c) to shield service providers—defined according to section 512(k)(1)(B)'s generous standard—from monetary liability for "direct, vicarious and contributory infringement for storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider."[123] The safe harbor applies in any "forum in which material may be posted at the direction of users."[124] Congress provides a list of examples of services that qualify for section 512(c) safe harbor—"providing server space for a user's web site, for a chatroom, or other forum in which material may be posted at the direction of users"—that indicates that it intended section 512(c) to cover a very wide range of services.[125]

Service providers must comply with a number of procedural formalities—over and above section 512(i) threshold requirements for all of

---

Caching (2000), *available at* http://www.cisco.com/warp/public/cc/pd/cxsr/00/tech/cds_wp.pdf.

118. *See* 17 U.S.C. § 512(b)(1), (2)(A)–(D) (2002); *see also* S. REP. No. 105-190, at 42–43 (1998) (discussing requirements for section 512(b) safe harbor).

119. *See* 17 U.S.C. § 512(b)(2)(E). For details of formal notifications of infringing activity, see discussion of section 512(c)(3) notifications *infra* Part II.A.iv.

120. *See* 17 U.S.C. § 512(b)(2)(E)(i).

121. *See id.* § 512(b)(2)(E)(ii).

122. *See id.* § 512(b)(2)(E).

123. S. REP. No. 105-190, at 43 (1998); *see also* 17 U.S.C. § 512(c)(1).

124. S. REP. No. 105-190, at 43.

125. *Id.*

section 512's safe harbors—to qualify for section 512(c) protection. They must appoint an agent to receive notifications of claimed infringement and provide contact information for the agent to the Register of Copyrights.[126] They must act expeditiously to disable access to infringing material on receipt of a notice of claimed infringement.[127] They must also take steps to assist any party that provides a designated agent a defective notice of claimed infringement to bring the notice into compliance with the requirements of section 512(c)(3)(A).[128]

Section 512(c), like the *Netcom* standard, includes a substantial and explicit knowledge element.[129] A service provider must remove or disable access to any infringing material on its network once it acquires actual or constructive knowledge of the material or activity using the material.[130] Constructive knowledge is broadly defined for purposes of section 512(c) as awareness of "facts or circumstances from which infringing activity is apparent."[131] Congress provides no examples of what sort of "facts or circumstances" would allow imputation of constructive knowledge of infringement to a service provider beyond stating that "if the service provider becomes aware of a 'red flag' from which infringing activity is apparent, it will lose the limitation of liability if it takes no action."[132] The red flag test for constructive knowledge has both subjective and objective elements.[133] The subjective element is subjective knowledge of the facts defined as a red flag on the part of the service provider.[134] The objective element is the definition of those facts; a red flag is any indication that would make infringing activity apparent to a reasonable person operating under similar circumstances.[135] Section 512(c) imposes a duty on service providers to disable access to any material they

126. *See* 17 U.S.C. § 512(c)(2).

127. *See* 17 U.S.C. § 512(c)(1)(C).

128. *See* 17 U.S.C. § 512(c)(3)(B)(ii). A detailed discussion of the contradictory intricacies of the section 512(c)(3) notice process is beyond the scope of this Note.

129. *Compare* 17 U.S.C. § 512(c)(i)–(ii), *with* Religious Tech. Ctr. v. Netcom, Inc., 907 F. Supp. 1361, 1374 (N.D. Cal. 1995) (noting that Netcom will be exposed to contributory liability if it had knowledge of user's infringement).

130. *See* 17 U.S.C. § 512(c)(1)(A)(i)–(iii); *see also* S. REP. No. 105-190, at 44 (1998) (noting that expeditious removal of material on acquiring actual or constructive knowledge necessary to preserve liability protection).

131. *See* 17 U.S.C. § 512(c)(1)(A)(ii).

132. *See* S. REP. No. 105-190, at 44 (1998).

133. *See id.*

134. *See id.*

135. *See id.*

actually know to be infringing or which passes the red flag test in order to preserve their safe harbor.[136]

Under these circumstances, a service provider's knowledge of infringing activity may expand in three ways:

1. its actual knowledge of infringing activity on its network will expand as its agents gain information about infringing material present on the network;[137] and
2. its subjective constructive knowledge will expand as its agents gain information about communications traffic on its network;[138] and
3. its objective constructive knowledge will expand as "reasonable persons" gain information about the patterns of user conduct and traffic that make infringing activity apparent.[139]

Together, these three aspects of the knowledge element of section 512(c) safe harbor expose service providers to a rapid expansion of their level of knowledge, actual and constructive, of infringement and thus to a dimunition of the extent of activity covered by the safe harbor.

The knowledge elements of section 512(c) coexist uncomfortably with Congress's intention to impose no duty on ISPs and other service providers affirmatively to police their networks for infringing material: "[A] service provider need not monitor its service or affirmatively seek facts indicating infringing activity . . . in order to claim this limitation on liability (or, indeed any other limitation provided by this legislation)."[140] Congress's intention is embodied in section 512(m)(1), which explicitly states that none of the safe harbor provisions shall be construed to require "monitoring [of] service or affirmatively seeking facts indicating infringing activity."[141]

v. Requirements for Section 512(d) Safe Harbor

Section 512(d) shields service providers—again, defined broadly according to section 512(k)(1)(B)—from monetary liability for copyright infringement for linking users to an Internet location

136. *See id.* at 45 ("A service provider wishing to benefit from the limitation on liability under subsection (c) must 'take down' or disable access to infringing material residing on its system or network of which it has actual knowledge or that meets the 'red flag' test, even if the copyright owner or its agent does not notify it of a claimed infringement.").

137. *See* discussion *supra* note 129 and accompanying text.

138. *See* discussion *supra* note 133 and accompanying text.

139. *See* discussion *supra* note 134 and accompanying text.

140. S. REP. No. 105-190, at 44.

141. 17 U.S.C. § 512(m)(1) (2002).

containing infringing material.[142] This safe harbor covers a broad range of activity, from the creation of directory services and search engines to hypertext linking.[143]

The section 512(d) safe harbor is subject to the same knowledge elements as section 512(c).[144] A service provider that gains actual or constructive knowledge of infringing material or activity must "remove, or disable access to" the material to preserve its section 512(d) safe harbor.[145] The service provider must also respond to notifications of claimed infringement by disabling access to allegedly infringing material.[146]

While Congress does not discuss in detail the level of actual or constructive knowledge required to disqualify a service provider from protection under section 512(c), it discusses the level of knowledge required to defeat a claim to section 512(d) protection extensively.[147] Because Congress provides so little guidance on the standard for establishing actual or constructive knowledge under section 512(c), its remarks regarding the knowledge standard imposed in section 512(d) are worth quoting at length:

> Like the information storage safe harbor in section 512(c), a service provider would qualify for [the section 512(d)] safe harbor if, among other requirements, it 'does not have actual knowledge that the material or activity is infringing' or, in the absence of such actual knowledge, it is 'not aware of facts or circumstances from which infringing activity is apparent.' Under this standard, a service provider would have no obligation to seek out copyright infringement, but it would not qualify for the safe harbor if it had turned a blind eye to 'red flags' of obvious infringement.

---

142. *See id.* § 512(d).

143. *See id*; *see also* S. REP. NO. 105-190, at 47 ("The term information location tools includes, for example: a directory or index of online sites or material such as a search engine that identifies pages by specified criteria, a reference to other online material such as a list of recommended sites, a pointer that stands for an Internet location or address, or a hypertext link which allows users to access material without entering its address.").

144. *See* 17 U.S.C. § 512(d)(1)(A)–(C); *see also* S. REP. NO. 105-190, at 47 (describing duty of service provider to remove infringing material on acquiring actual or constructive knowledge of the infringement).

145. 17 U.S.C. § 512(d)(1)(A); *see also* S. REP. NO. 105-190, at 47 (noting correspondence between notice provisions of section 512(c) and (d)). Oddly, section 512(d) includes no requirement that a service provider appoint an agent to receive notifications of alleged infringement. No case law has yet addressed the question of whether a service provider may avail itself of the section 512(d) safe harbor without appointing an agent.

146. 17 U.S.C. § 512(d)(1)(A); *see also* S. REP. NO. 105-190, at 47.

147. *See* S. REP. NO. 105-190, at 48–49.

For instance, the copyright owner could show that the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was clearly, at the time the directory provider viewed it, a 'pirate' site of the type described below, where sound recordings, software, movies or books were available for unauthorized downloading, public performance or public display. Absent such 'red flags' or actual knowledge, a directory provider would not be similarly aware merely because it saw one or more well known photographs of a celebrity at a site devoted to that person. The provider could not be expected, during the course of its brief cataloguing visit, to determine whether the photograph was still protected by copyright or was in the public domain; if the photograph was still protected by copyright, whether the use was licensed; and if the use was not licensed, whether it was permitted under the fair use doctrine.

The important intended objective of this standard is to exclude sophisticated 'pirate' directories—which refer Internet users to other selected Internet sites where pirate software, books, movies, and music can be downloaded or transmitted—from the safe harbor. Such pirate directories refer Internet users to sites that are obviously infringing because they typically use words such as 'pirate,' 'bootleg,' or slang terms in their uniform resource locator (URL) and header information to make their illegal purpose obvious to the pirate directories and other Internet users. Because the infringing nature of such sites would be apparent from even a brief and casual viewing, safe harbor status for a provider that views such a site and then establishes a link to it would not be appropriate. Pirate directories do not follow the routine business practices of legitimate service providers preparing directories, and thus evidence that they have viewed the infringing site may be all that is available for copyright owners to rebut their claim to a safe harbor.

In this way, the 'red flag' test in section 512(d) strikes the right balance. The common-sense result of this 'red flag' test is that online editors and catalogers would not be required to make discriminating judgments about potential copyright infringement. If, however, an Internet site is obviously pirate, then seeing it may be all that is needed for the service provider to encounter a

'red flag.' A provider proceeding in the face of such a red flag must do so without the benefit of a safe harbor.[148]

Congress intended that mere awareness on the part of the ISP or its agent of activity or material—without knowledge of its infringing nature—not suffice to deprive the provider of the section 512(d) safe harbor.[149] Congress did not assume that ISPs were experts in copyright law and therefore refused to impute to them the ability to measure the infringing character of particular activities in the absence of a glaring "red flag."[150] Congress's goal in limiting the extent of constructive knowledge was to preserve human-compiled search engines from secondary liability imposed on the sole basis of a single cataloging visit.[151]

At the same time, Congress provided indications that providing access to obviously infringing material would be sufficient, under some circumstances, to establish constructive knowledge and defeat the ISP's section 512(d) safe harbor.[152] If the ISP links a user to a "pirate site," the copyright holder will be able to establish the ISP had at least constructive knowledge of copyright infringement.[153] Beyond enumerating some patterns of conduct associated with "pirate sites" like using the strings "pirate" or "bootleg" in their URLs and distributing obviously unlicensed copyright material, Congress provides no guidance on the boundary between a "pirate site"—viewing which will deprive an ISP of its section 512(d) safe harbor—and an infringing but non-pirate site—which an ISP may safely view without sacrificing its protection from liability.[154]

vi. Section 512(h) Infringer-Identification Subpoenas

Section 512(h) allows a copyright owner or its authorized agent to seek a subpoena requiring a service provider to identify an alleged infringer without filing a claim against the infringer.[155] In order for the

148. *See id.*

149. *See id.* at 49.

150. *Id.* at 48.

151. *See id.* at 49 (1998) (discussing value to Internet user of human-compiled search engines like Yahoo! and interest in preserving human editorial role to reduce exposure to "irrelevant and offensive material").

152. *See id.* at 48 (1998) (discussing plaintiffs' ability to establish constructive knowledge by showing ISP's awareness of "red flags" or "pirate sites").

153. *See id.*

154. Congress's notion of a "pirate site" appears to correspond closely to "warez" sites, which distribute unlicensed versions of commercial software or provides easy access to locations where such software is available. *See, e.g.,* http://www.warez.com/; http://www.easydownloads.net/.

155. 17 U.S.C. § 512(h) (2002).

subpoena to issue, the copyright owner must submit a copy of the notification it has provided—or will provide—to the service provider under section 512(c)(3)(A), a copy of the proposed subpoena, and a declaration attesting to its good faith in seeking the alleged infringer's identity.[156] If all of the owners' materials are in order, Congress intended that "the issuing of the order should be a ministerial function performed quickly."[157] Congress also intended that section 512(h) infringer-identification subpoenas would only be available to copyright owners "who have submitted or will submit a . . . notification satisfying the requirements of subsection (c)(3)(A)."[158]

Since section 512(a) has no knowledge element in determining an ISP's monetary liability and makes no reference to notification at all while section 512(b), (c), and (d) include a knowledge element and refer to notification, Congress did not intend section 512(h) to authorize subpoenas where an ISP is engaged in transmission or routing of others' messages.[159] The only Federal appellate court that has addressed the issue adopted this analysis, holding that section 512(h) infringer-identification subpoenas are not available where an ISP's activity is protected by the section 512(a) safe harbor.[160]

vii. Section 512(j) Limitations on Injunctive Relief

While section 512(a)–(d) limits service providers' monetary liability for copyright infringement, section 512(j) limits the scope of injunctive relief available to copyright holders.[161] If an ISP qualifies for the section 512(a) transmission and routing safe harbor, injunctive relief is limited to suspension of a "subscriber or account holder['s]" access to the ISP's network or reasonable steps to block access to a "specific, identified, online location outside the United States."[162] Congress appears to have intended that injunctive relief in section 512(a) situations would be available only to ISPs which had a direct contractual relationship with the infringing end user, since other ISPs in the web of mutual message

156. *Id.* § 512(h)(2)(A)–(C).
157. S. REP. No. 105-190, at 51.
158. *Id.*
159. *Compare* 17 U.S.C. § 512(a) *with* section 512(b)–(d); *see also* discussion *supra* Part II.B.
160. *See* Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1237 (D.C. Cir. Dec. 19, 2003) (noting that cross-references to section 512(c)(3)(A) notification provisions in sections 512(b) and (d) and lack of such cross references in section 512(a) support conclusion that section 512(h) subpoenas unavailable for activity covered by section 512(a) safe harbor).
161. *See* 17 U.S.C. § 512(j).
162. *See id.* § 512(j)(1)(B).

forwarding will not have a subscription relationship with the end user and will therefore have no account to terminate.[163]

If the section 512(b), (c), or (d) safe harbors apply, the court's power to grant injunctive relief is less limited.[164] The court may order the service provider to suspend a subscriber's access to its services or to prevent access to "a particular online site on the provider's system or network."[165] The court may also impose any other injunctive relief it considers necessary, if these steps are "the least burdensome to the service provider among the forms of relief comparably effective for that purpose."[166]

However the court characterizes the ISP's activity, it must take the following four factors into account in shaping injunctive relief:

> (A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;
>
> (B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;
>
> (C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and
>
> (D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.[167]

These factors require the court to balance the ISP's interest in efficient operation of its networks—factors (A), (C), and (D)—against the potential harm the copyright owner may suffer—factor (B).[168] Research

---

163. *See id.* Congress makes the same assumption of a contractual relationship between the end user in Senate Report 190. *See* S. REP. No. 105-190, at 53 (1998) (observing that injunctive relief available when ISP activity covered by section 512(a) safe harbor limited to "an order to the service provider to terminate subscriber accounts that are specified in the order").

164. *See* 17 U.S.C. § 512(j)(1)(A).

165. *See id.* § 512(j)(1)(A)(i), (ii).

166. *See id.* § 512(j)(1)(A)(iii).

167. *Id.* § 512(j)(2).

168. *See id.*.

reveals no court that has yet addressed the implications of these limitations on injunctive relief.[169]

B. *The Section 512 Safe Harbor Provisions as a Whole*

Taken in its entirety, section 512 creates a complex scheme of statutory safe harbors from liability for service providers:

(1) SECTION 512(A) SAFE HARBOR FOR ISP MESSAGE FORWARDING: ISPs and other network connectivity providers are entitled to a safe harbor from monetary liability analogous to common carrier protection for the automatic transmission of messages *regardless of their knowledge* of the content of the messages.[170] In addition, section 512(h) infringer-identification subpoenas are unavailable and section 512(j) limits injunctive relief to termination of a subscriber's account or suspension of access to a network resource outside U.S. jurisdiction.[171]

(2) SECTION 512(B) SAFE HARBOR FOR NETWORK CACHING: All service providers are entitled to safe harbor from monetary liability for local caching of material to facilitate efficient distribution *regardless of their knowledge* of the content of the material, so long as they abide by minimal notification requirements.[172] Section 512(h) subpoenas are available and only section 512(j)(1)(A)'s limits on injunctive relief apply.[173]

(3) SECTION 512(C) SAFE HARBOR FOR USER-DIRECTED STORAGE: All service providers are entitled to safe harbor from liability for storing material at the direction of a user *so long as they have neither actual nor constructive knowledge of user's infringement* and abide by the notification requirements of section 512(c)(1)(c).[174] Section 512(c) corresponds closely with the rule enunciated in *Netcom* because it shields an ISP from direct liability for forwarding messages that infringe copyright but leaves open the possibility that ISP may be a contributory infringer if it had actual or constructive knowledge of the infringement.[175]

---

169. *Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1235 (D.C. Cir. Dec. 19, 2003), appears to be the only discussion of section 512(j) in any published Federal decision. The court makes reference to section 512(j)(1)(A)'s distinction between "providing access to material" and "terminating the account of [a] subscriber" to support its conclusion that no notification of claimed infringement delivered by a copyright owner to an ISP engaged in section 512(a) transmission or routing can substantially meet the requirements of section 512(c)(3)(A)(iii), which requires such notifications to include sufficient information to allow the ISP to disable access to the material. *Id.*

170. *See* discussion *supra* Part II.A.ii.

171. See 17 U.S.C. § 512(a), (h), (j); *see also* discussion *supra* Part II.A.

172. *See* discussion *supra* Part II.A.iii.

173. See 17 U.S.C. § 512(a), (h), (j); *see also* discussion *supra* Part II.A.

174. *See* discussion *supra* Part II.A.iv.

175. *Compare* Religious Tech. Ctr. v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361, 1373–75 (N.D. Cal. 1995), *with* 17 U.S.C. § 512(c)(1)(A).

As with section 512(b), section 512(h) subpoenas are available and section 512(j)(1)(A)'s limits on injunctive relief apply.[176]

(4) SECTION 512(D) SAFE HARBOR FOR INFORMATION LOCATION TOOLS: All service providers are entitled to safe harbor from liability for providing an index or other link to infringing material *so long as they have neither actual nor constructive knowledge of infringing nature of the material* and abide by the notification requirements of section 512(d)(1)(c).[177] As with sections 512(b) and (d), section 512(h) subpoenas are available and section 512(j)(1)(A)'s limits on injunctive relief apply.[178]

The section 512(a) safe harbor, as demonstrated above, is easily the most robust. It includes no knowledge element in assessing monetary liability, shields the ISP from section 512(h) subpoenas, and limits injunctive relief, in practical terms, to termination of a subscriber's account.[179] The other safe harbors are substantially less safe: a service provider may be monetarily liable if it has actual or constructive knowledge of the infringing activity, section 512(h) subpoenas are available, and courts have broad discretion in shaping injunctive relief for copyright owners.[180]

The section 512 liability protection regime, therefore, requires courts to characterize a service provider's activity before determining which safe harbor applies. The court's characterization will shape the outcome of the litigation, since the availability of monetary damages, injunctive relief and section 512(h) infringer-identification subpoenas all depend on it. Despite the importance of characterization, Congress provided little guidance of courts, either in section 512 itself or in the legislative history. Section 512(n) explicitly states that the safe harbors of section 512(a)–(d) apply independently of each other; a particular entity may qualify for safe harbor under all, some, or none of the subsections, based solely on the criteria within each subsection.[181] Congress clearly anticipated that particular service providers would engage in activity that would implicate several of the safe harbors:

> Section 512's limitations on liability are based on functions, and each limitation is intended to describe a separate and distinct function. Consider, for example, a service provider that provides

176. See 17 U.S.C. § 512(a), (h), (j); *see also* discussion *supra* Part II.A.
177. *See* discussion *supra* Part II.A.v.
178. *See* 17 U.S.C. § 512(a), (h), (j); *see also* discussion *supra* Part II.A.
179. *See* discussion *supra* Part II.A.ii.
180. *See* discussion *supra* Parts II.A.iii–v.
181. *See* 17 U.S.C. § 512(n).

> a hyperlink to a site containing infringing material which it then caches on its system in order to facilitate access to it by its users. This service provider is engaging in at least three functions that may be subject to the limitation on liability: transitory digital network communications under subsection (a), system caching under subsection (b), and information locating tools under subsection (d).[182]

Despite clearly anticipating the overlapping effect of the safe harbors, Congress made no provision for resolving ambiguity regarding characterization of activities, beyond implying that the plaintiff's characterization of the activity in the complaint will determine which safe harbor applies.[183]

C. *A Rejected Alternative: House Bill 2281 Section 202*

The elaborate characterization scheme in section 512 does far more than codify *Netcom*. The legislative history of section 512 demonstrates that Congress intended to extend protection to ISPs beyond that offered in *Netcom*.[184] Congress considered and rejected the option of simply adopting the *Netcom* rule shielding ISPs from direct liability for passive or automatic transmission of messages but leaving open the possibility of contributory or vicarious liability.[185] Statements in the House Report indicating that section 512 "essentially codifies the result in the leading and most thoughtful judicial decision to date: [*Netcom*]" refer to language not included in the DMCA as finally passed.[186] The House Report on the DMCA, House Report 551, instead, refers to the text of the version of section 512 that passed the House:

> a) LIMITATION- Notwithstanding the provisions of [17 U.S.C.] section 106, a provider shall not be liable for—
>
> (1) direct infringement, based solely on the intermediate storage and transmission of material through a system or network controlled or operated by or for that provider, if—
>
> (A) the transmission was initiated by another person;

---

182. H.R. REP. No. 105-551, pt.2, at 65 (1998).

183. *Id.* (suggesting that details of complaint determine applicability of individual safe harbors).

184. For an extended treatment of the legislative history of the DMCA, see David Nimmer, *Appreciating Legislative History The Sweet And Sour Spots Of The DMCA's Commentary*, 23 CARDOZO L. REV. 909 (2002).

185. *See* discussion *infra* Part II.C.

186. *See* H.R. REP. No. 105-551, pt. 1 at 11, 24–26 (1998).

(B) the storage and transmission is carried out through an automatic technological process, without any selection of that material by the provider; and

(C) no copy of the material thereby made by the provider is maintained on the provider's system or network in a manner ordinarily accessible to anyone other than the recipients anticipated by the person who initiated the transmission, and no such copy is maintained on the system or network in a manner ordinarily accessible to such recipients for a longer period than is reasonably necessary for the transmission;

(2) monetary relief under section 504 or 505 for contributory infringement or vicarious liability, based solely on conduct described in paragraph (1).

3) monetary relief under section 504 or 505 for contributory infringement or vicarious liability, based solely on transmitting or providing access to material over that provider's system or network, other than conduct described in paragraph (1), if the provider—

(A) does not have actual knowledge that the material is infringing or, in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; and

(B) does not receive a financial benefit directly attributable to the infringing activity, if the provider has the right and ability to control such activity.[187]

In this form, the bill lacks most of the features of the final version of section 512, including:

(1) the quadripartite characterization system contained in section 512(a)–(d);[188]

(2) the bifurcated definitions of service provider contained in section 512(k)(1);[189]

187. H.R. 2281, 105th Cong. § 202 (1998).

188. *Compare* H.R. 2281 § 202(a) (describing service provider liability protection without reference to characterization beyond single category of "intermediate storage and transmission"), *with* 17 U.S.C. § 512(a)–(d) (2002) (defining section 512 safe harbors and requiring characterization of activity).

189. *Compare* H.R. 2281 § 202(a), *with* 17 U.S.C. § 512(k)(1).

(3) infringer-identification subpoenas available under section 512(h);[190] and

(4) the limitations on injunctive relief imposed in section 512(j).[191]

Equally importantly, the version of the bill described in the House Report distinguishes between direct liability and contributory infringement and vicarious liability.[192] In section 512(a)(1) of that version, service providers were shielded from all liability for direct infringement when they automatically stored or transmitted others' messages without selecting their content, provided that they do not retain a copy of the message.[193] Section 512(a)(2) of that version shielded them from monetary liability for contributory infringement or vicarious liability, subject to the same conditions.[194] This explicit distinction between direct liability and contributory or vicarious liability is not present in section 512 as finally passed.[195]

The House Report refers to section 512(a)(1) as a shield from direct infringement and section 512(a)(2) as a shield from contributory and vicarious infringement; the final version of section 512 does not address these issues in these sections—and does not mention contributory or vicarious infringement at all. The version reported in the House includes these provisions in the appropriate sections, making it evident that the House Report's comments concern a version of section 512 that Congress considered and rejected.[196]

The House Report is therefore of extremely limited value in determining Congress's final intent in enacting section 512, since it comments on a text never adopted into law.[197] Section 512's protections for ISPs—especially the quasi-common carrier protections offered in section 512(a)—extend beyond the *Netcom* rule barring direct liability. Other provisions, such as section 512(b)–(d) may leave open the possibility of contributory liability but they are more extensive than the protection offered by House Bill 2281, the mere codification of *Netcom* that Congress considered and rejected.[198]

---

190. *Compare* H.R. 2281 § 202(a), *with* 17 U.S.C. § 512(h).
191. *Compare* H.R. 2281 § 202(a), *with* 17 U.S.C. § 512(j).
192. *See* H.R. 2281 § 202(a).
193. *Id.*
194. *Id.*
195. *See* 17 U.S.C. § 512.
196. *Compare* H.R. 2281 § 202(a), *with* 17 U.S.C. § 512.
197. *See* H.R. 2281 § 202(a).
198. *See* discussion *supra* Part II.B.

In its final form, section 512(a) provides ISPs with robust protection from monetary liability for end users' infringement, freedom from section 512(h) subpoenas, and limitations on the injunctive relief available to copyright owners. The section 512(a) safe harbor, however, is only available if courts are willing to characterize the ISP's activity as section 512(a) transmission or routing as opposed to section 512(c) storage of information at the direction of a user which lacks such robust protection. Part II will argue that courts have had difficulty characterizing particular ISP activities and have therefore struggled to apply section 512 consistently with Congress's intent.

III. CHARACTERIZATION: DEFINING AN ISP'S ACTIVITY AND EXPOSURE TO LIABILITY

Given the limited direction available, courts have not found a consistent standard for characterizing particular Internet activities. Characterization of an activity will often determine the outcome of a claim against a service provider since bringing an activity into the section 512(a) safe harbor excludes consideration of ISP knowledge of infringing activity, bars section 512(h) subpoenas, and limits injunctive relief under section 512(j).[199] The section 512 (b), (c), and (d) safe harbors impose none of these restrictions.[200] The exclusion of consideration of the ISP's level of knowledge is particularly important because courts have reached widely varying conclusions regarding the level of knowledge that constitutes a "red flag" that allows a plaintiff to establish that an ISP has constructive knowledge of infringement on the part of a user.[201] Usenet—the mutual message-forwarding network whose technical characteristics are discussed *supra* Part I.B.ii—is a particularly appropriate case study for examining courts' difficulty in characterizing particular activities according to the section 512 categories. First, the technical characteristics of Usenet allow it, under certain circumstances, to satisfy the requirements of each of the section 512(a), (b), and (c) safe harbors. Second, Federal courts have already characterized it as both a section 512(a) service and a section 512(c) service.[202] Part III.A will

199. *See* discussion *supra* Part II.B.

200. *See* discussion *supra* Part II.B.

201. *See* discussion *infra* Part IV.A.

202. *Compare* Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., 907 F. Supp. 1361, 1372–74 (N.D. Cal. 1995) (establishing principle of limited liability for ISPs and including analysis of ISP's knowledge in evaluation of liability), *and* ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 623 (4th Cir. 2001) (characterizing Usenet service offered by Usenet specialist provider as section 512(c) activity with knowledge element), *with* Ellison

outline Usenet's technical characteristics and argue that these characteristics allow Usenet arguably to fit into several of section 512's categories. Part III.B will argue that the 4th Circuit incorrectly characterized an ISP's participation in Usenet as a section 512(c) activity in *ALS Scan, Inc. v. RemarQ Communities, Inc.*[203] and that the District Court for the Central District of California correctly characterized it as a section 512(a) activity in *Ellison v. Robertson.*[204]

A. *Usenet's Technical Characteristics and Section 512*

Characterizing activity on the Internet according to the categories provided in section 512 is a difficult task at a purely factual level. Usenet is particularly difficult to characterize because it is an early example of distributed peer-to-peer networking, but one in which ISPs (and in some cases, other service providers) own and control the computers that participate in the peer-to-peer network.[205] Usenet's peer-to-peer architecture reduces demands on long-distance transmission capacity by distributing messages throughout the network of servers so that end users can retrieve any message directly from a local server without consuming long-distance transmission capacity.[206] Its peer-to-peer architecture also means that no single server exercises control over Usenet as a whole; there is no central authority.[207]

Usenet, therefore, possesses technical characteristics that allow courts to characterize it as section 512(a) transitory network communications—if the service provider in question meets the section 512(k)(1)(A) definition required to qualify for section 512(a) protection—section 512(b) system caching, or section 512(c) information residing on systems at the discretion of users.

Usenet fits the requirements of the section 512(a) safe harbor in that:

(1) end users initiate transmission of Usenet messages; and

(2) Usenet servers forward end-user-initiated messages according to automated technical processes without specific selection of the content of the messages; and

---

v. Robertson, 189 F. Supp. 2d 1051 (C.D. Cal. 2002) (characterizing Usenet service offered by ISP as section 512(a) activity without knowledge element).

203. *ALS Scan*, 239 F.3d at 619.

204. *Ellison*, 189 F. Supp.2d at 1051. Mr. Ellison has appealed the District Court's grant of summary judgment to AOL to the United States Court of Appeals for the Ninth Circuit. Oral arguments took place March 6, 2003. *See* Ellison v. AOL, Inc., No. 02-55797 (9th Cir. argued Mar. 6, 2003).

205. *See* WIKIPEDIA, THE FREE ENCYCLOPEDIA, *Usenet*, *at* http://en2.wikipedia.org/wiki/Usenet (last updated Dec 3, 2003) (characterizing Usenet as peer-to-peer application).

206. *Id.*

207. *Id.*

(3) recipient end users request the messages they wish to read; and

(4) ISPs' Usenet servers store end users' messages for only a limited time; and

(5) ISPs generally do not modify the content of end users' messages.[208]

Though no court has yet raised the possibility, Usenet also fits the requirements of the section 512(b) safe harbor since:

(1) the mutual message forwarding system requires the "intermediate and temporary storage of material [newsgroup postings] on a system or network controlled or operated by or for the service provider";

(2) end users initiate transmission of Usenet messages;

(3) Usenet messages reach end users of many other ISPs; and

(4) ISPs retain copies of Usenet messages through an automatic technical process for the purpose of making the messages available to their end users.[209]

While Congress appears to have drafted section 512(b) on the assumption that it would primarily apply to so-called "web caches" the provision is drafted in general terms and does not exclude ISP activity that creates local caches for material distributed using other networking protocols.[210]

Usenet also fits the broader requirements of the section 512(c) safe harbor—"[(1)] storage [(2)] at the direction of a user [(3)] of material [(4)] that resides on a system or network [(5)] controlled or operated by or for the service provider"[211]— in that:

(1) ISPs' Usenet servers retain end users' messages for some period of time; such retention could be characterized as "storage"; and

(2) end users initiate the messages; and

---

208. *See* discussion *supra* Part I.B.iii.

209. *See* discussion *supra* Part I.B.iii.

210. *See* S. REP. No. 105-190, at 42–43 (1998) (combining general references to caching technology with specific references to "popular sites" and "originating sites"). For additional discussion of web caching technology, see *supra* note 116 and accompanying text.

211. 17 U.S.C. § 512(c) (2002) (numbering added for clarity of reference).

(3) end users' messages may include material that infringes copyright and

(4) retention of these messages as part of the forwarding process will lead the material in the messages to reside on a system—the Usenet server;[212] and

(5) ISPs' Usenet servers will either fall under their control or be operated for their benefit.[213]

The text of section 512 provides no particular criteria for determining which characterization is correct, though the section 512(a) safe harbor is only available to "[entities] offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received,"[214] a definition that will apply to ISPs as well as to other communications service providers. Congress' intent to increase the level of liability protection available to ISPs beyond that offered by the *Netcom* doctrine, however, provides strong support for the proposition that courts should apply the section 512(a) safe harbor to any activity that might be characterized as subject either to section 512(a) or section 512(c). If any activity that may be characterized as section 512(a) activity or section 512(c) activity is subject only to section 512(c)'s limited protection, Congress's clear intent to extend protection to ISPs beyond *Netcom's* limited bounds will be frustrated.[215]

B. *The Legal Dispute Over Characterization of Usenet*

Two post-DMCA cases have characterized ISP participation in the Usenet message-forwarding system under section 512: *ALS Scan*[216] and *Ellison*.[217] In *ALS Scan*, the Fourth Circuit characterized providing Usenet service to end users as a section 512(c) activity; in *Ellison*, a Federal

212. *See* discussion *supra* Part I.B.iii. Even if the materials do not "reside" on a system, the inclusion of a "network" as a potential location for user-initiated material to reside makes it likely that Usenet will satisfy this element of the section 512(c) safe harbor.

213. *See* discussion *supra* Part I.B.iii. Many ISPs outsource Usenet services to specialty Usenet providers; these providers give ISPs' end users direct access to a Usenet server operated by the specialty provider. These servers may be collocated with servers belonging to the ISP and both parties may share administrative roles on the server; such arrangements would satisfy all elements of the "controlled or operated by or for the service provider" language.

214. 17 U.S.C. § 512(k)(1)(A) (2002).

215. *See* discussion *supra* Parts II.B, II.C.

216. ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001).

217. Ellison v. Robertson, 189 F. Supp. 2d 1051 (C.D. Cal. 2002).

District Court characterized it as a section 512(a) activity.[218] The *ALS Scan* court relied on the superseded House Report on the version of section 512 that Congress considered and rejected and therefore drew the mistaken conclusion that section 512 merely codified *Netcom*.[219] *Ellison*, however, applies section 512 consistently with Congress's intent and characterizes Usenet service as a section 512(a) activity subject to all the robust liability protections Congress intended to provide to ISPs.[220]

i. *ALS Scan*: Usenet as a Section 512(c) Activity

In *ALS Scan*, a copyright holder brought a copyright infringement claim against a specialty Usenet service provider, RemarQ.[221] RemarQ provided Usenet service to end users and ISPs.[222] RemarQ also participated as a peer in the Usenet peer-to-peer network, forwarding messages to peer servers according to algorithms defined by RemarQ staff.[223] RemarQ did not monitor or otherwise control content in any Usenet newsgroup.[224] It did, however, have the technical capacity to deny access to particular newsgroups to particular users or to configure its servers to refuse messages from particular newsgroups or based on other criteria.[225] RemarQ stored incoming Usenet messages for "8–10 days" before deleting them to conserve storage space.[226]

Based on these facts, the Fourth Circuit concluded that RemarQ's provision of Usenet services fell under the section 512(c) safe harbor for information residing on systems or networks at the direction of users without meaningful discussion of how it reached its conclusion.[227] The

218. *Compare Ellison*, 189 F. Supp. at 1072, *appeal docketed*, No. 02-55797 (9th Cir. argued Mar. 6, 2003) (applying section 512(a)), *with ALS Scan*, 239 F.3d at 623 (applying section 512(c)).

219. *See ALS Scan* 239 F.3d at 622 (referring to House Report explicating language excluded from final version of section 512); *see also* discussion *supra* Part II.C.

220. *See Ellison*, 189 F. Supp. 2d at 1069 n.19 (carefully vetting language of H.R. Rep. No. 105-551, pt. I at 24 to determine Congressional intent).

221. *ALS Scan*, 239 F.3d at 621. The Court characterized RemarQ as an "Internet service provider" without tying that characterization to an assessment of RemarQ's compliance with the section 512(k)(1)(A) requirements for eligibility for the section 512(a) safe harbor. RemarQ, now known as Supernews, remains active in the Usenet service outsourcing field; it provides service both to individuals and to other ISPs. For further details, see *Supernews Company Information*, *at* http://www.supernews.com/compinfo.html (last visited Nov. 27, 2003).

222. *Als Scan*, 239 F.3d at 621.

223. *Id.*

224. *See id.*

225. *Id.* These technical capabilities are common to all peer participants in Usenet.

226. *Id.*

227. *See id.* at 623 ("The liability-limiting provision applicable here, 17 U.S.C. § 512(c) . . . .").

court did not address the possibility that RemarQ might meet the section 512(k)(1)(A) requirements for safe harbor under section 512(a) or that its Usenet services might qualify for section 512(a) safe harbor.[228] RemarQ does not appear to have argued that it was entitled to section 512(a) safe harbor, choosing instead to seek section 512(c) safe harbor by describing itself as a " 'host' to persons and entities."[229]

The court's characterization of Usenet services as a section 512(c) activity brought RemarQ's level of knowledge regarding users' infringing activity and the adequacy of its response to ALS Scan's notices into question, exposing RemarQ to contributory liability for mere participation as a peer in Usenet's automated message-forwarding system.[230] ALS Scan did not allege infringement by any end users of RemarQ's services or ISPs to whom it provided services.[231] The court reasoned, based on the superseded House Report, that section 512 as a whole merely codified *Netcom* and that therefore RemarQ, like Netcom, was shielded from direct liability for its passive or automatic acts but might still be liable on a contributory theory if it had knowledge of the infringement.[232] The court reaches the same substantive result that application of the Netcom rule would have produced, but it misses Congress's intent to extend the protections of section 512 substantially

---

228. *Id.* The Fourth Circuit appears to miss the distinction between the section 512(k)(1)(A) requirements for section 512(a) safe harbor and the far less restrictive requirements of section 512(k)(1)(B) which apply to sections 512(b), (c), and (d). *See id.* at 623 (conflating section 512(k)(1)(B) and section 512(k)(1)(A) definitions of service provider, and noting that neither side contests RemarQ's status as an "Internet service provider," without specifying whether this RemarQ meets the section 512(k)(1)(A) requirements for section 512(a) safe harbor). Had the Fourth Circuit directly addressed the issue, it might have concluded that RemarQ did not, in fact, meet the requirements of section 512(k)(1)(A) and was therefore not entitled to the section 512(a) safe harbor. Research reveals no court that has yet addressed the issue of specialist Usenet service providers' ability to avail themselves of the section 512(a) safe harbor in a published decision. RemarQ, as a Usenet provider, is not as easily defined as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user" as, for example, AOL or Verizon. RemarQ, however, since it merely provides access to Usenet servers which forward end users' messages to other servers in the mutual message forwarding network, could certainly argue that it is providing transmission and routing services to its users and other service providers. Congress drafted the definition of service provider for section 512(a) purposes in section 512(k)(1)(A) at a high level of abstraction and did not explicitly exclude entities like RemarQ.

229. Appellant's Brief at 4, ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001) (No. 00-1351), *available at* 2000 WL 33991307.

230. *See* ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 623 (4th Cir. 2001) (noting that sections 512(c)(1)(A)(i)–(ii) requirement that ISP lack actual or constructive knowledge of infringing material or activity central to section 512(c) analysis).

231. *Id.* at 621.

232. *See id.* at 622 (citing language in H.R. REP. NO. 105-551, pt. 1 indicating that section 512 "essentially codifies [*Netcom*]").

beyond the limits established in *Netcom* and embodied in the early version the House Report describes.[233]

The Fourth Circuit bases its conclusion that section 512 merely codifies *Netcom* on language from House Report 551, pt. 1, that stresses service providers' exposure to contributory liability for automated transmissions on the *Netcom* model; as demonstrated *supra* Part II.C, this language refers to provisions of the then-pending bill that were superseded by the final version of section 512(a) and is therefore irrelevant.[234] The court also cites House Conference Report 796,[235] the Conference Committee Report on the final version of the DMCA, but the page cited includes only the unhelpful statement that "Title II preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[236] So general a statement of Congress's intent provides very little basis for the court's characterization of participation in Usenet as a section 512(c) activity, with all the exposure to liability that characterization creates, especially given the very next sentence in the Conference Committee Report: "At the same time, [section 512] provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."[237]

ii. *Ellison*: Usenet as a Section 512(a) Activity

In *Ellison*, Harlan Ellison, a noted science fiction writer, brought copyright infringement claims against several providers of Usenet services, including AOL and RemarQ.[238] The claims against the ISPs were

---

233. *See id.* at 622 (noting that "the ultimate conclusion on [the direct infringement] point is controlled by Congress's codification of the *Netcom* principles in Title II of the DMCA").

234. *Id.* at 622 (discussion of legislative history of DMCA referring to superseded version of section 512(a)); *see also* discussion *supra* Part II.C. This language appears in a section immediately preceding the court's analysis of RemarQ's exposure to liability under section 512; while directly addressed at refuting plaintiff's claim that RemarQ was liable for direct infringement under the *Frena* doctrine entirely rejected in the DMCA, it provides important background regarding the court's general assumptions regarding ISPs' liability for users' activity that infringes copyright.

235. H.R. CONF. REP. NO. 105-796 (1998).

236. H.R. CONF. REP. NO. 105-796, at 72; *see also ALS Scan*, 239 F.3d at 625 (citing H.R. CONF. REP. NO. 105-796, at 72).

237. H.R. CONF. REP. NO. 105-796, at 72.

238. *See* Ellison v. Robertson, 189 F. Supp. 2d 1051, 1054–55 (C.D. Cal. 2002); *remanded for further fact-finding on other grounds*, 357 F.3d 1072 (9th Cir., 2004) (remanding for fact-finding regarding AOL's satisfaction of section 512(i) threshold requirements for section 512(a)–(d) safe harbors but explicitly adopting District Court's characterization of Usenet as section 512(a) activity).

based solely on their role in automatically forwarding allegedly infringing Usenet messages to other participants in the Usenet network.[239] Plaintiff later dismissed RemarQ from the case, but RemarQ's activities—participating as a peer in Usenet's automated message-forwarding network—were identical to the activities at issue in *ALS Scan*.[240] AOL's participation in the Usenet network was functionally identical to RemarQ's activities in *ALS Scan* except that AOL retained Usenet messages with binary content[241] on its servers for "approximately fourteen days."[242]

The *Ellison* court, in contrast to the Fourth Circuit, characterized AOL's participation as a peer in the Usenet message-forwarding system as "transitory digital network communications" entitled to safe harbor under section 512(a).[243] In doing so, the court concluded that the threshold requirements of section 512(k)(1)(A) limiting eligibility for section 512(a) safe harbor to "[entities] offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received" merely restated the substantive provisions of section 512(a), allowing it to bypass an extensive discussion of AOL's status as a section 512(k)(1)(A) service provider.[244] The court found that AOL's participation as a peer in Usenet met all the elements of the section 512(a) safe harbor:

(1) other persons initiated transmission of the messages;[245] and

(2) AOL played no role in selecting the infringing material for distribution;[246] and

(3) AOL played no role in selecting the recipients of the material;[247] and

---

239. *See id.*

240. *See id.* at 1055 (noting settlement between plaintiff and RemarQ).

241. Binary content includes graphics files, audio files, motion picture files, and compiled computer programs, among other categories. Many Usenet peer servers retain messages with binary content for shorter periods of time than text messages because they occupy more storage space on the server.

242. *Ellison*, 189 F. Supp. 2d at 1054.

243. *Id.* at 1067–68.

244. *See id.* at 1068. In practical terms, however, it is difficult to imagine that AOL would not qualify as a service provider under section 512(k)(1)(A) under any circumstances where it was providing access to Internet resources as opposed to its own proprietary resources.

245. *See id.* at 1071.

246. *See id.*

247. *Id.* at 1071–72.

(4) AOL stored the messages for only fourteen days, no longer that was "reasonably necessary for the transmission, routing, or provision of connections;"[248] and

(5) AOL did not modify the content of the messages.[249]

The court rejected Ellison's claim that the automated filtering rules that AOL had applied—it is the rare ISP that carries every single Usenet newsgroup, and AOL certainly did not—constituted "selection of the material" under section 512(a)(2).[250] The court reasoned that if automatic filtering barred ISPs from the section 512(a) safe harbor, ISPs would be forced either to abandon their filtering practices—and therefore carry newsgroups for which there was no end user demand as well as newsgroups devoted to criminal practices like child pornography and prostitution—or abandon their section 512(a) liability protection.[251] Given Congress's oft-expressed concern with protecting minors from illegal obscene content online, the court refused to require ISPs to forward patently criminal messages in order to retain their section 512(a) safe harbor.[252]

In reaching its conclusion, the court relied to some extent on House Report 551, pt. 1, though it noted the substantial differences between the text examined in the House Report and the final text of section 512.[253] The court limited its reliance on the House Report to determining that Congress intended section 512(a)(4) to allow ISPs to store material for whatever period of time—even two weeks, as in this case—might be reasonably necessary for transmission.[254]

The court based this conclusion on the fact that both the earlier version of section 512 described in the House Report and the final version of section 512 used the language exempting service providers from liability when they transmit or route communications and "no [intermediate] copy is maintained on the [service provider's] system or

248. *See id.* at 1070 (discussing retention of messages in context of the eleven-day retention period in *Netcom* and Congress's intent expressed in H.R. REP. NO. 105-551, pt. I at p. 24 to adopt the holding in *Netcom*). See discussion *supra* Part II.C for an extensive discussion of the limitations of this report as a source of legislative history of the DMCA.

249. *See Ellison*, 189 F. Supp. 2d at 1072.

250. *See id.* at 1071 (holding that service provider's selection of newsgroups to carry does not qualify as selection of material under section 512(a)(2)).

251. *Id.* (noting that economic and police power interests support interpretation of section 512(a) that allows ISPs to engage in automated selection of Usenet traffic for forwarding).

252. *Id.*

253. *Id.* at 1069 (noting discrepancy between text analyzed in House Report and final text and commenting on difficulties of using superseded legislative history).

254. *See id.* (detailing analysis of House Report's commentary on analogous language from superseded version of section 512).

network . . . for a longer period than is reasonably necessary for the transmission."[255] The court reasoned that if this language remained in the final version of section 512, the House Report's assertion that Congress intended this language to mean that "intermediate copies may be retained without liability for only a limited period of time" remained relevant.[256] The court also concluded that if the House Report remained relevant on this issue, then its assertion that *Netcom* defined the limits of "a limited period of time" for section 512 purposes also remained relevant.[257] Based on these premises, the court finally concluded that if eleven days' storage qualified as a limited period of time under *Netcom*'s facts, then AOL's fourteen-day retention period must meet section 512(a)(4)'s *Netcom*-derived standard.[258]

The Ellison court read section 512's legislative history correctly.[259] In contrast to the *ALS Scan* court, it carefully determined which elements of the legislative history related to language that entered the final version of the statute and ignored elements of the legislative history concerning versions of the statute that Congress considered and rejected.[260] The Ninth Circuit recently remanded the case to the District Court for further fact-finding on the issue of AOL's compliance with section 512(i)'s threshold requirements for the section 512(a)–(d) safe harbors.[261] In doing so, the Ninth Circuit explicitly adopted the District Court's section 512(a) characterization, stating that:

> If after remand a jury finds AOL to be eligible under section 512(i) to assert the safe harbor limitations of sections 512(a–d), the parties need not relitigate whether AOL qualifies for the limitation of liability provided by section 512(a); the district

255. *Compare* H.R. 2281, 105th Cong. § 202(a) (1998), *with* 17 U.S.C. § 512(a)(4) (2002).

256. *Ellison*, 189 F. Supp. 2d at 1070, *citing* H.R. Rep. 105-551, pt. 1, at p. 24 ("By referring to temporary storage of copies, *Netcom* recognizes implicitly that intermediate copies may be retained without liability for only a limited period of time. The requirement in paragraph 512(a)(1) that 'no copy [be] maintained on the system or network . . . for a longer period than reasonably necessary for the transmission' is drawn from the facts of the *Netcom* case, and is intended to codify this implicit limitation in the *Netcom* holding.

257. *Ellison*, 189 F. Supp. 2d at 1070.

258. *See id.*.

259. *See* Ellison v. Robertson, 357 F.3d 1072, 1072 (9th Cir. 2004).

260. *Compare* Ellison v. Robertson, 189 F. Supp. 2d 1051, 1069-70 (C.D. Cal. 2002) (carefully separating superseded elements of House Report from elements that retain relevance), *with* ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 662 (4th Cir. 2001) (accepting language in House Report stating that version of section 512 that Congress considered and rejected merely codified *Netcom*).

261. *See* Ellison v. Robertson, 357 F.3d 1072, 1072 (9th Cir. 2004).

court's resolution of that issue at the summary judgment stage is sound.[262]

iii. *Ellison*'s Section 512(a) Characterization is More Consistent with Congress's Intent

The *Ellison* court's characterization of AOL's participation in Usenet as section 512(a) transmission or routing is more consistent with Congress' intent in adopting section 512 than is the Fourth Circuit's characterization in *ALS Scan* of RemarQ's participation in the same network as storage of material at the direction of a user subject to section 512(c).[263] The Fourth Circuit erred by accepting as authoritative language in the House Report that refers to a version of section 512 that Congress considered and rejected before passing section 512 in its final form. The Fourth Circuit, misled by the superseded legislative history, therefore ignored the stronger protections for transmission and routing activity that Congress inserted into section 512 after the House Report was complete.[264]

Instead of applying section 512's statutory safe harbor scheme, the Fourth Circuit chose to treat section 512 as a mere codification of *Netcom*.[265] As extensively demonstrated above, section 512's text and the legislative history of its final form strongly support the conclusion that it is a substantial extension of *Netcom*.[266] The Fourth Circuit ignored section 512's characterization scheme in favor of mechanical application of *Netcom*; in doing so, the court may have served the interests of judicial economy—section 512's interdependent provisions are not easy to parse—but it misread both the text and the legislative history of section 512.[267]

The *Ellison* court, by contrast, understood that section 512's nested scheme of safe harbors provided substantially greater protection from liability to ISPs than did *Netcom*.[268] It applied the statute as written, with proper reference to the small sections of the House Report which had not been rendered irrelevant by revisions in section 512.[269] Most importantly, the court took seriously Congress's decision to create in section 512(a) a

---

262. *Id.*
263. *See* discussion *supra* Parts III.B.i, III.B.ii.
264. *See* discussion *supra* Parts II.C, III.B.i.
265. *See* discussion *supra* Parts II.B, III.B.i.
266. *See* discussion *supra* Parts II.B, II.C.
267. *See* discussion *supra* Parts II.B, II.C, III.B.i.
268. *See* discussion *supra* Part III.B.ii; *see also* Ellison v. Robertson, 189 F. Supp. 2d 1051, 1064–72 (C.D. Cal. 2002) (extensively discussing AOL's compliance with statutory requirements of section 512(a) safe harbor).
269. *See* discussion *supra* Part III.B.iii.

quasi-common carrier safe harbor for entities that transmit and rout messages on the Internet.[270] The *Ellison* court was therefore correct when it characterized an ISP's participation in the Usenet network as transmission or routing activity entitled to the section 512(a) safe harbor.

IV. CHARACTERIZATION AND ITS CONSEQUENCES

Courts' inconsistent characterization of Usenet in *ALS Scan* and *Ellison* shows the importance of characterization of ISPs' activity in determining the outcome of copyright infringement claims. A court's characterization of an ISP's activity for section 512 purposes will determine:

(1) the availability of monetary relief for contributory infringement;[271]

(2) the availability of section 512(h) intruder-identification subpoenas;[272] and

(3) the extent of injunctive relief available to the plaintiff.[273]

In each of these areas, the ISP benefits greatly if the court characterizes its activity as transmission or routing shielded by section 512(a)'s quasi-common-carrier protections. The copyright owner, for its part, is substantially more likely to prevail—and to gain the monetary damages and broad injunctive relief it seeks—if the court characterizes the ISP's activity as storage at the direction of a user entitled only to the section 512(c) safe harbor.

While Usenet is an interesting case study that reveals the importance of characterization for section 512 purposes, the characterization issue is likely to arise in cases that seek to hold ISPs and other service providers liable for providing access to other peer-to-peer networks. Kazaa, Grokster, and Gnutella are prominent examples of peer-to-peer networks.[274] If providing access to these networks qualifies as section 512(a) transmission or routing, then ISPs are not liable on either direct or contributory theories for infringing activity over these networks. If, however, courts

270. *See* discussion *supra* Parts II.B, III.B.ii–iii]; *see also Ellison*, 189 F. Supp. 2d at 1054–55 (discussing implications of section 512(a)–(d) statutory safe harbors).

271. *See* discussion *supra* Parts I.A, II.B.

272. *See* discussion *supra* Parts II.A.vi, II.B.

273. *See* discussion *supra* Parts II.A.vii, II.B.

274. Details of these second-generation peer-to-peer technologies are provided in *Metro-Goldwyn Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1031–33 (C.D. Cal. 2003) (detailing technical characteristics of peer-to-peer technologies).

define these activities as "storage at the direction of a user" "on a system or network controlled or operated by or for the service provider" governed by section 512(c), the ISP may be liable on a contributory theory if it had actual or constructive knowledge of the infringing material or activity.

The court's characterization of the activity in question, therefore, will shape the entire development of the litigation.[275] Part IV.A will argue that ISPs are very likely to prevail in litigation if the court characterizes the activity in question as transmission or routing subject to the section 512(a) safe harbor. Part IV.B will argue that uncertainty regarding courts' characterization of particular activities will have a chilling effect on ISPs' willingness to support—or even tolerate—the emergence of new networking technologies. Part IV.C will urge courts to take ISP activity characterization seriously and to allow ISPs to avail themselves of the section 512(a) transmission and routing safe harbor when appropriate.

A. *Legal Consequences*

If courts adopt the *ALS Scan* analysis and conclude that participation in Usenet—or other similar mutual message forwarding systems—is section 512(c) storage at the direction of a user in order to reach a substantive result analogous to the outcome in *Netcom*, ISPs:

(1) will be exposed to contributory liability for any Usenet message that infringes copyright if they have actual or constructive knowledge of the infringement;[276]

(2) will be required to comply with section 512(h) infringer-identification subpoenas;[277] and

(3) will be subject to a broad range of injunctive relief under section 512(j)(1)(A).[278]

By contrast, if courts adopt the *Ellison* analysis, defining participation in Usenet or similar systems as section 512(a) transmission or routing, ISPs:

(1) will be preserved from all monetary liability for Usenet users' copyright infringement, regardless of their level of knowledge;[279]

---

275. *See* discussion *infra* Part IV.A.
276. *See* discussion *supra* Parts I.A, II.B.
277. *See* discussion *supra* Parts II.A.vi, II.B.
278. *See* discussion *supra* Parts II.A.vii, II.B.
279. *See* discussion *supra* Parts II.A.ii, II.B.

(2) will not be subject to section 512(h) infringer-identification subpoenas;[280] and

(3) will benefit from strict limits on injunctive relief under section 512(j)(1)(B).[281]

The most important consequence of a court's characterization decision is that section 512(a) shields an ISP from contributory liability for its activity while section 512(c) does not.[282] The outcome in *Ellison* demonstrates this distinction clearly. Since section 512(a) does not include a knowledge element, the court found that AOL was shielded from all liability for copyright infringement, regardless of its knowledge or lack thereof regarding the particular infringement in question *even though* plaintiff had raised issues of material fact regarding AOL's actual knowledge of the infringements in question.[283] This outcome demonstrates section 512(a)'s ability to shield ISPs from contributory—in addition to direct—liability for users' copyright infringement.[284]

By contrast, section 512(c)'s safe harbor is only available if an ISP has neither actual nor constructive knowledge of the infringement.[285] As the *ALS Scan* court put it, "[section 512(c)] immunity, however, is not presumptive, but granted only to 'innocent' service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under the three prongs of 17 U.S.C. § 512(c)(1)."[286] An ISP will lose its section 512(c) safe harbor by failing to prove its "innocence" of the infringement long before a copyright holder can establish the knowledge element of its contributory infringement claim.[287] *ALS Scan* provides an example of this limitation of the section 512(c) safe harbor.[288] ALS Scan's notification of claimed infringement and allegations that RemarQ had actual knowledge of particular infringements of

280. *See* discussion *supra* Parts II.A.vi, II.B.

281. *See* discussion *supra* Parts II.A.vii, II.B. ISPs, of course, can only avail themselves of section 512(a)'s robust protection if they meet section 512(k)(1)(A)'s threshold definition of service provider.

282. *See* discussion *supra* Part II.A.ii.

283. *See* Ellison v. Robertson, 189 F. Supp. 2d 1051, 1071–72 (C.D. Cal. 2002) (finding AOL protected from monetary liability under section 512(a)); *id.* at 1059 (finding that plaintiff has raised material question of fact regarding AOL's willful ignorance of infringements in question).

284. *See supra* note 279 and accompanying text.

285. *See* 17 U.S.C. § 512(c)(1)(A)(i)–(ii) (2002).

286. ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 625 (4th Cir. 2001).

287. *See id.* at 625–26 (holding that service provider that could not prove ignorance of infringement was not entitled to section 512(c) safe harbor while expressing doubts about copyright owner's prospects of proving knowledge element of contributory infringement).

288. *See id.*

ALS Scan copyrights were enough to deny RemarQ access to the section 512(c) safe harbor but not enough to hold it liable as a contributory infringer.[289] In any case where a plaintiff can establish the knowledge element of contributory infringement, section 512(c) is unlikely to provide a shield from liability, since the ISP's knowledge will deny it safe harbor under either section 512(c)(1)(A)(i) or section 512(c)(1)(A)(ii).[290] It is therefore an uncertain shield against claims of contributory infringement.

The court's characterization of ISP activity will also determine whether section 512(h) infringer-identification subpoenas are available to copyright owners.[291] *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.*,[292] the only published Federal appellate decision to address the issue, establishes a simple rule: section 512(h) subpoenas are available if the ISP engages in section 512(b) system caching, section 512(c) storage at the direction of a user, or section 512(d) provision of information location tools, but not for section 512(a) transmission and routing.[293] Under this rule, if a court characterizes an activity as section 512(a) transmission or routing, a copyright owner must file a claim—and not merely allege copyright infringement—in order to gain access to the court's subpoena power.[294] Under these circumstances, ISPs are likely to be subject to substantially smaller subpoena-compliance burdens if their activity fits the section 512(a) safe harbor than if it falls into section 512(c).

---

289. *See id.*

290. *See* 17 U.S.C. § 512(c)(1)(A)(i)–(ii) (2002); *see also* discussion *supra* Part II.A.iv. Research revealed no published case in which a court has ruled on this issue when an ISP is involved. Courts which have denied non-ISP service providers the section 512(c) safe harbor have preferred instead to focus on shortcomings of the providers' compliance with section 512(i)'s threshold requirements for any of the safe harbors or with the notice requirements of section 512(c). *See, e.g.*, Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1175–81 (C.D. Cal. 2002) (discussing at length age verification service provider's failure to comply with section 512(c) and (i) requirements); Costar Group Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688, 703–04 (D. Md. 2001) (declining to extend section 512(c) safe harbor to web hosting service on grounds that material questions of fact exist regarding its section 512(c) and (i) compliance).

291. *See* discussion *supra* Part II.A.vi.

292. Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003).

293. *Id.* at 1236.

294. *See* FED. R. CIV. P. 45(a)(1)(B) (requiring that subpoena state title of pending action); *see also, e.g.*, United States v. Morton Salt Co., 338 U.S. 632, 641–42 (1950) ("Federal judicial power itself extends only to adjudication of cases and controversies and it is natural that its investigative powers should be jealously confined to these ends.").

Finally, the court's characterization of ISP activity will determine the extent of injunctive relief available to the copyright owner.[295] If the court characterizes the activity as section 512(a) transmission or routing, section 512(j)(1)(B) limits injunctive relief to an order to terminate the direct infringer's account or block access to a specific online location outside U.S. jurisdiction.[296] If the activity falls into the section 512(c) safe harbor, the copyright owner faces much looser limits on the injunctive relief available.[297]

Taken together, these legal disadvantages place an ISP whose activities are accorded only the section 512(c) safe harbor in a difficult position. Because the ISP's level of knowledge of the infringing activity remains relevant to assessing liability, the ISP is subject to expensive and intrusive discovery aimed at its officers and employees.[298] In addition, the ISP has very little guidance regarding what sort of actual or constructive knowledge will defeat its section 512(c) safe harbor under section 512(c)(1)(A)(i) and (ii). An ISP would have to feel confident indeed to put itself to the test under the proof of innocence standard the Fourth Circuit enunciated in *ALS Scan*.[299] Under these circumstances, an ISP is far less likely to prevail against a claim of copyright infringement if the court characterizes its activity as section 512(c) storage than if it qualifies as section 512(a) transmission or routing.[300]

B. *Practical Consequences*

The practical consequences of uncertainty over ISP access to the robust quasi-common-carrier protection of the section 512(a) transmission and routing safe harbor are substantial. First, exposure to monetary liability, section 512(h) subpoenas, and extensive injunctive relief may induce an ISP to settle a case if it fears that it will only benefit from the section 512(c) safe harbor. RemarQ appears to have made exactly this calculation in *Ellison*.[301] In exchange for Mr. Ellison's agreement to drop

---

295. *See* discussion *supra* Part II.A.vii.

296. *See* discussion *supra* Part II.A.vii.

297. *See* 17 U.S.C. § 512(j)(1)(A) (2002); *see also* discussion *supra* Part II.A.vii.

298. *See* ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 626 (4th Cir. 2001) (remanding case to District Court for "further development of the record" on purpose of particular newsgroups identified in ALS Scan's notification).

299. *See ALS Scan*, 239 F.3d at 625 (holding that section 512(c) safe harbor "granted only to 'innocent' providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three prongs of 17 U.S.C. § 512(c)(1)").

300. *Compare* Ellison v. Robertson, 189 F. Supp. 2d 1051, 1072 (C.D. Cal. 2002) (applying section 512(a)), *with ALS Scan*, 239 F.3d at 623 (applying section 512(c)).

301. *See Ellison*, 189 F. Supp. 2d at 1055 (noting that Mr. Ellison dismissed RemarQ from case on January 18, 2002). A somewhat disjointed press release narrating some of the

the suit and to forego any claims for monetary damages, RemarQ agreed to develop software that allowed Mr. Ellison to delete postings he judged to be infringing and to provide access to an employee to assist him in deleting the postings if necessary.[302] The settlement demonstrates RemarQ's concern that the section 512(c) safe harbor would not shield it from liability; the terms of the settlement allow Mr. Ellison to exert some degree of control over RemarQ's business and would be entirely unworkable if they applied to every copyright owner.[303]

Second, uncertainty regarding exposure to liability may affect ISPs' willingness to tolerate the presence of new networking applications on their networks or to forward others' messages. ISPs cannot be confident that participation in automated message-forwarding networks like Usenet or providing network resources that users use to connect to more modern peer-to-peer networks will be characterized as section 512(a) transitory digital network communications and not section 512(c) storage of material on a system or network controlled or operated by the ISP.[304]

So far, only one Federal appellate court has held on the issue of characterization of peer-to-peer networking systems for section 512 pur-

---

details of the case from the point of view of Mr. Ellison's supporters is available at http://harlanellison.com/KICK/kick_rls.htm. This account indicates that RemarQ had not entered into settlement talks with Mr. Ellison before the Fourth Circuit decided *ALS Scan*. *See* Press Release, Harlan Ellison and Critical Path, Inc. (Jan. 19, 2002), *available at* http://harlanellison.com/KICK/crit_rls.htm (last visited Jan. 5, 2004).

302. *See id.* The press release reads as follows:

> The copyright infringement action filed by noted author and literary activist Harlan Ellison against Critical Path, Inc. and its subsidiary RemarQ Communites, Inc. has been settled. The action stemmed from the unauthorized posting of some of Ellison's most well-known copyrighted stories on the RemarQ service. Ellison's copyright infringement action is continuing against the remaining defendant, America Online, Inc.
>
> Among the terms of the settlement, Critical Path will develop software that allows Ellison immediately to delete unauthorized postings of his works of which he becomes aware. Critical Path will also appoint an employee to be available to Ellison as a back up measure.
>
> Ellison, who has authored 75 books in his distinguished career, noted: "I am pleased to have settled this case with Critical Path and RemarQ and believe we have taken a step forward for writers everywhere in their efforts to protect copyrighted works."
>
> The settlement did not include any admission of liability. Commenting on the settlement, a Critical Path spokesperson said: "We are pleased to reach a settlement in this case that will aid authors in protecting their intellectual property."

Id.

303. *See id.*

304. *See* 17 U.S.C. § 512(a), (c) (2002).

poses. In Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc,[305] the District Court of the District of Columbia found that peer-to-peer networks running over an ISP's network qualified as transitory digital network communications for section 512(a) purposes.[306] This characterization, however, came in the context of a the court's refusal to allow section 512(h) infringer-identification subpoenas to issue where an ISP's activities fall within the section 512(a) safe harbor and not in an assessment of an ISP's exposure to liability for a user's copyright infringement.[307] The decision also calls into question the continued applicability of *Ellison's* characterization of participation in Usenet as section 512(a) transmission or routing. The court's rationale for characterizing peer-to-peer file sharing by an ISP's users as section 512(a) transmission or routing rested on a bright line distinction between "an ISP storing infringing material on its servers in any capacity"—entitled to one of the section 512(b)–(d) safe harbors—and "an ISP routing infringing material to or from a personal computer owned and used by a subscriber"—entitled to section 512(a) safe harbor.[308] This bright line rule is easier to administer than the complex analysis required in *Ellison*, but it risks exposing an ISP to liability whenever infringing material resides on a computer under its control long enough to be in "storage."[309] If other courts follow the *Verizon* court by excluding any ISP activity that includes storage of files on ISP-owner equipment "in any capacity," ISPs may be entitled only to the section 512(c) safe harbor for participating in Usenet and similar message-forwarding systems that involve temporary storage of messages on an ISP's servers.

In addition, the *Verizon* court's characterization of an ISP carrying peer-to-peer networking traffic as subject to the section 512(a) safe harbor is not justified at any particular length in the decision.[310] Other courts have not yet reached the issue of ISP liability for carrying peer-to-peer

---

305. Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1233 (D.C. Cir. 2003).

306. *See id.* (characterizing ISP as "only . . . a conduit for data transferred between two [I]nternet users" and applying section 512(a) safe harbor in subsequent analysis).

307. *See id.* at 1236 (ruling that copyright holders are not entitled to section 512(h) subpoenas to identify users when ISP engaged in section 512(a) activities).

308. *Id.* at 1237.

309. Defining the period of "storage" required to place an ISP in the section 512(c) safe harbor as opposed to section 512(a) will be difficult in any case, since section 512(a)'s safe harbor includes protection for "intermediate and transient storage." 17 U.S.C. § 512(a), (c) (2002). *Ellison* makes a reasonable argument that storage of material for up to fourteen days can qualify as "intermediate and transient" under certain circumstances. *See* Ellison v. Robertson, 189 F. Supp. 2d 1051, 1068–70 (C.D. Cal. 2002); *see also* discussion *supra* Part III.B.ii.

310. *Verizon*, 351 F.3d at 1233 (characterizing Verizon as "conduit for P2P file sharing" entitled to section 512(a) safe harbor without further elaboration).

file sharing traffic, but there is a realistic possibility that they will not choose to follow *Verizon* on the issue, especially given copyright owners' strong interest in convincing courts to characterize such activity as section 512(c) storage at the direction of a user.[311] Copyright owners can argue that the text of section 512(c)—referring to "material that resides on a system or *network* controlled or operated by or for the service provider" [emphasis added]—supports such a characterization.[312]

The *Verizon* court adopted the District Court's conclusion that "[b]ecause peer-to-peer users most often swap materials over the Internet that are stored on their own computers—not on the service providers' networks—such activity is within subsection (a), not subsection (c)."[313] This characterization, however, is not essential to the District Court's holding, since the District Court concluded that section 512(h) subpoenas were available to copyright owners regardless of which section 512 safe harbor protected the ISP's activity.[314] In addition, the District Court ignored the possibility that information can reside on a *network* controlled or operated by or for the service provider without residing on a *system* controlled or operated by or for the service provider.[315] The District Court treats information as resident on a service provider's network only if it resides on a system under the service provider's control.[316] This interpretation renders the term "network" in section 512(c) superfluous, violating a standard rule of statutory construction. The conclusion that information residing on users' systems connected to a service provider's network resides on the network is equally plausible and does not raise the same difficulties of statutory construction as the District Court's interpretation. Copyright owners can also plausibly argue that the *Verizon* court's characterization thwarts Congress' intent in enacting section 512 by effectively shielding the vast majority of infringing communication over the Internet from any action by copyright owners short of a legal claim.[317] *Verizon's* limited treatment of characterization has not disposed of these arguments.

---

311. See discussion *supra* Part IV.A for an elaboration of the legal advantages that accrue to a copyright owner if the court characterizes an ISP's activity as subject to the section 512(c) safe harbor.

312. *See* 17 U.S.C. § 512(c) (2002).

313. In re Verizon Internet Services, Inc., 240 F. Supp. 2d 24, 35 (D. D.C. 2003).

314. *See id.* at 44.

315. *See id.* at 35.

316. *See id.*

317. For examples of this sort of argument, see *In re Verizon*, 240 F. Supp. 2d at 36–39 (noting incongruity of shielding peer-to-peer file sharing from copyright owners' section 512(h) subpoena power).

ISPs may choose to react to this uncertainty by reducing their exposure through technical means. If ISPs do not know whether participation in Usenet is entitled to the section 512(a) safe harbor, they may suspend their participation in mutual message forwarding systems like Usenet, or at least reduce the number of newsgroups which they carry in order to avoid exposure to litigation. No ISP wishes to suffer the fate of RemarQ: expensive legal defeat followed by rapid settlement of other claims. To the extent that ISPs are unsure how courts will characterize other networking technologies, they will have an incentive to use bandwidth management and security tools to prevent network activity associated with networking technologies that may expose them to liability on their networks.[318]

The easiest way to do so is by forbidding categories of traffic that the ISP does not approve, a practice common on corporate networks.[319] Newly-developed hardware and software tools allow networking professionals to monitor and prioritize particular categories of traffic. Some of these tools, like the Packeteer PacketShaper[320] and the Allot NetEnforcer,[321] are intended primarily to allow networking professionals to maximize the efficiency of traffic flow on their networks. Others, like the Symantec Gateway Security appliance[322] and the Check Point Enterprise Suite with Floodgate-1[323] combine traffic-management features with highly-developed security-management tools. Widespread deployment of these tools will slow development of new network applications; these applications will fail, at least initially, to function at all.[324]

---

318. *See, e.g.*, Julia King, *Preventing P2P Abuse*, COMPUTERWORLD, Dec. 8, 2003, at 52 (describing University of Florida's development of automated system to detect peer-to-peer applications and disable network access for computers on which they reside); Parry Aftab, *What To Do Before The RIAA Knocks*, INFORMATIONWEEK, Oct. 6, 2003 (advising businesses and universities to eliminate peer-to-peer applications from their networks to avoid liability).

319. Businesses and universities often deploy security devices known as firewalls to protect their networks and monitor incoming and outgoing traffic. These devices and a new category of device that prioritizes particular categories of traffic give organizations substantial control over end users' ability to use particular networking applications.

320. Full details of Packeteer's products are available at http://www.packeteer.com/ (last visited November 15, 2003).

321. Full details of Allot's products are available at http://www.allot.com/ (last visited November 15, 2003).

322. Symantec provides details of the Gateway Security 5400 series at http:// enterprisesecurity.symantec.com/products/products.cfm?ProductID=133. Product cycles in the security industry are sufficiently short that several generations of this category of product will have come and gone before this Note reaches publication.

323. Check Point offers both hardware appliances and software products in this category. Full details of their offerings are available at http://www.checkpoint.com/.

324. *See, e.g.*, David Margulius, *Blockers, spammers, and domain name overlords threaten universal Internet connectivity*, INFOWORLD, Nov. 24, 2003, at 42. Developers may find means of circumventing network management tools, but their efforts will simply renew an

If large ISPs implement this strategy throughout their networks in order to reduce their exposure to liability—or for other reasons—they will also convert their networks into immediate and automated mechanisms of control. They will have a level of control over communication and commerce that exceeds even Jeremy Bentham's dreams for the Panopticon. In place of potential surveillance, they will impose immediate, pervasive, and automated control. The settlement that RemarQ reached in *Ellison* could extend to a service provider's entire network; copyright owners would gain veto power over communication or at least convert ISPs' networks into instrumentalities for preserving their rights.[325]

Some ISPs, including several academic institutions, have already instituted such automated monitoring. The University of Florida, for example, has created a software tool called ICARUS that monitors traffic over its network, identifies traffic that appears to be characteristic of peer-to-peer file sharing, and then suspends network service to the computer generating the traffic for 30 minutes.[326] Users may regain network access only if they complete a 10-minute interactive presentation on copyright law.[327] As of November 22, 2003, the author of the tool had received inquiries "from more than 110 universities, eight Internet service providers and 23 companies" seeking information on how to deploy similar monitoring and control solutions on their networks.[328] The Joint Committee of the Higher Education and Entertainment Communities, composed of leaders from the higher education community and music and motion picture industries, studied ICARUS as a potential solution for controlling file sharing at other universities.[329]

Now that this level of fine-grained, automatic control over users' communications is available to ISPs, the Internet is no longer an undifferentiable cloud but an automated Panopticon. ISPs have the ability to allow or disallow communications according to extremely sophisticated rules with only a limited investment of time, money and effort. Section

---

arms race between network management development and novel application development. The same cycle of repression and response occurs at a legal level. For a discussion of changes in the development of peer-to-peer software in response to legal developments, see Timothy Wu, *When Code Isn't Law*, 89 VIRGINIA L. REV. 679 (2003).

325. *See supra* note 300 and accompanying text.

326. *See* Ron Word, *University's Software Kicks Off Downloaders*, HOUSTON CHRONICLE, Nov. 22, 2003, *available at* http://www.chron.com/ cs/CDA/ssistory.mpl/tech/news/2242112.

327. *Id.*

328. *Id.*

329. *See* Katie Dean, *Florida Dorms Lock Out P2P Users*, WIRED NEWS, Oct. 3, 2003, *available at* http://www.wired.com/news/digiwood/0,1412,60613,00.html (last visited Nov. 27, 2003). For further details on the Joint Committee of the Higher Education and Entertainment Communities, see JCHEEC, *Request For Information #2 Frequently Asked Questions*, *at* http://www.educause.edu/asp/faq/faq.asp?Code=RFI2.

512(a)'s quasi-common-carrier protection for transmission and routing shields ISPs from copyright owners' pressure to convert their networks into instrumentalities of monitoring and control.[330] If placing this sort of control in copyright owners hands is desirable, society should make that decision openly and explicitly instead of allowing such pervasive control to emerge from the messy legal struggle between ISPs and copyright holders.

In the case of conventional telecommunications, society acted to bar telecommunications providers from taking advantage of their control of the instrumentalities of communication to control their users' behavior by forbidding them to monitor or control communications and shielding them from liability for communications over their networks.[331] Section 512(a) provides similar protections for Internet communications, shielding ISPs from most liability for transmitting messages and users from casual identification by copyright owners.[332] If society chooses to apply a different regime to ISPs, that decision should only be made after careful consideration. The historical accident that led to the emergence of the confederation of networks that makes up the Internet has already provided enormous advantages to society; it would be tragic if the transformative potential of Internet communications disappeared in another historical accident.

Communications over the Internet should not be accorded a different level of protection from monitoring simply because they are easier to monitor. Judge Easterbrook's famous comment that there should no more be a law of cyberspace than there is a law of the horse must cut both ways.[333] "Technological advances must continually be evaluated and their relation to legal rules determined so that antiquated rules are not misapplied in modern settings. . . . Yet, if the substance of a transaction has not changed, new technology does not require a new legal rule merely because of its novelty."[334]

---

330. *See* discussion *supra* Parts IV.A, IV.B.

331. *See* discussion *supra* Part I.B.i.

332. *See* discussion *supra* Part IV.A.

333. *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996).

334. Daniel v. Dow Jones & Co., 520 N.Y.S.2d 334, 338 (N.Y.C. Civ. Ct. 1987).